THE CAPABILITIES OF THE U.S. GOVERNMENT TO COLLECT AND ANALYZE ECONOMIC INTELLIGENCE

A thesis presented to the Faculty of the U.S. Army Command and General Staff College in partial fulfillment of the requirements for the degree

MASTER OF MILITARY ART AND SCIENCE

by

ERICA BALLARD RUSSELL, MAJ, USA
B.A., University of Texas at Arlington, Arlington, Texas, 1979
M.A., University of Southern California, Los Angeles, California, 1983

Fort Leavenworth, Kansas
1994

Approved for public release; distribution is unlimited.

MASTER OF MILITARY ART AND SCIENCE

THESIS APPROVAL PAGE

Name of Candidate: MAJ Erica Ballard Russell

Thesis Title: The Capabilities of the U.S. Government to Collect and Analyze Economic Intelligence

Approved by:

Cyrus E. Holliday, Thesis Committee Chairman
MAJ Cyrus E. Holliday, M.A., M.S.

Nancy A. Morales, Member
LTC Nancy Morales, B.A.

Thomas K. Adams, Member
LTC Thomas K. Adams, Ph.D.

Robert W Duffner, Member, Consulting Faculty
COL Robert W. Duffner, Ph.D.

Accepted this 3rd day of June 1994 by:

Philip J. Brookes, Director, Graduate Degree Programs
Philip J. Brookes, Ph.D.

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the U.S. Army Command and General Staff College or any other governmental agency. (References to this study should include the foregoing statement.)

ABSTRACT

THE CAPABILITIES OF THE U.S. GOVERNMENT TO COLLECT AND ANALYZE ECONOMIC INTELLIGENCE by MAJ Erica Ballard Russell, USA, 118 pages.

This study investigates the capabilities of the United States Government to collect and analyze economic intelligence for possible use by U.S. corporations. Focusing predominantly on the U.S. Intelligence Community it reviews the missions, collection methods, and analytical responsibilities of the Central Intelligence Agency, Defense Intelligence Agency, National Security Agency, and other government entities with economic intelligence functions.

The study also reviews the relation between economic competitiveness and national security as articulated by the President and the Department of Defense. It discusses the role of foreign governments in conducting economic espionage for and providing economic intelligence to their own corporations to promote economic competitiveness. The capabilities of the U.S. Intelligence Community are described and evaluated against six criteria: accuracy, cost, releasability, suitability, target accessibility, and timeliness.

The study finds that the United States Government can collect and analyze economic intelligence that is usable by private U.S. industry. The Community would need to make some changes to focus on detailed industry information vice broad economic trends; internal assets would require redistribution to perform the mission.

TABLE OF CONTENTS

	Page
APPROVAL PAGE	ii
ABSTRACT	iii
LIST OF ILLUSTRATIONS	v
LIST OF ABBREVIATIONS	vi
CHAPTER	
1. INTRODUCTION	1
2. RESEARCH METHODOLOGY	15
3. FOREIGN GOVERNMENTS' ROLE IN ECONOMIC ESPIONAGE	21
4. THE U.S. INTELLIGENCE COMMUNITY	38
5. ANALYSIS OF U.S. GOVERNMENT'S CAPABILITIES	54
6. CONCLUSION	75
APPENDIX	
A. DEFINITIONS	81
B. MILITARILY CRITICAL TECHNOLOGIES	85
C. GOVERNMENT DOCUMENTS AVAILABLE	91
D. LITERATURE REVIEW	95
ENDNOTES	103
BIBLIOGRAPHY	113
INITIAL DISTRIBUTION LIST	118

LIST OF ILLUSTRATIONS

Tables

1. Market Share Percentage for High-Technology Manufacturers. 5

2. U.S. Companies Targeted by French Government for Industrial Espionage. 27

3. Technology Transfer Responsibilities. 52

4. U.S. Intelligence Community Budget. 65

5. Computer Technology: Foreign Technology Assessment Summary. 89

6. Telecommunications Technology: Foreign Technology Assessment Summary. 90

Figures

1. National Shares of Patents Granted in the U.S., by Country of Origin. 3

2. U.S. Intelligence Community. 40

LIST OF ABBREVIATIONS

CIA	Central Intelligence Agency
C^3I	Command, Control, Communications & Intelligence
CI	Competitive Intelligence
COMINT	Communications Intelligence
DCI	Director of Central Intelligence
DGSE	Direction General de la Securite Exterieure
DoD	Department of Defense
DIA	Defense Intelligence Agency
DUSD(IP)	Deputy Under Secretary of Defense (International Policy)
HPSCI	House Permanent Select Committee on Intelligence
HUMINT	Human Intelligence
IC	Intelligence Community (also USIC)
IDA	Institute for Defense Analyses
IMINT	Imagery Intelligence
JETRO	Japanese External Trade Organization
MCTL	Militarily Critical Technologies List
MITI	Ministry for International Trade and Industry (Japan)
NRO	National Reconnaissance Office
NSA	National Security Agency
NSD	National Security Directive
OSINT	Open Source Intelligence
S&TI	Scientific and Technical Intelligence
SSCI	Senate Select Committee on Intelligence
USDA	Under Secretary of Defense for Acquisitions
USG	United States Government

CHAPTER 1

INTRODUCTION

On 15 November 1991, President Bush issued National Security Directive (NSD) 29, in which he named economic competitiveness as a vital interest to U.S. national security. During his confirmation hearings in February 1993, Central Intelligence Agency (CIA) Director, James Woolsey said, "he would review how aggressively the CIA and other agencies should collect economic intelligence and how widely they should disseminate their findings among U.S. companies to help them combat foreign competitors."[1]

This change in policy was motivated by three factors: a perceived decline of U.S. economic competitiveness; the economic intelligence collection activities of foreign governments; and economic-related national security interests of the United States. Of the three factors, the one most discussed in U.S. Government and industry circles is economic espionage activities by allies. An economic espionage threat "originates from a variety of countries including France, Japan, Israel, India, Pakistan, South Korea, and Taiwan."[2]

This activity's importance lies in its potential to affect the other two named factors: the security and economic competitiveness of the United States. As Peter Schweizer describes in Friendly Spies, U.S. businesses are concerned that if they cannot protect their research and production abilities they will lose the motivation and profits for further development. Some individuals go even further to suggest that industry should not just protect its secrets but receive information on competitor foreign companies from the

United States Government (USG). Senator David Boren from Oklahoma suggests an approach in the middle: "We [the United States] should obtain information about the economic negotiation strategies of other countries and foreign competitors where possible. It is appropriate to use our intelligence assets to level the playing field and to allow American companies an equal chance to compete."[3]

Research Question

The primary question of this study is: Does the U.S. Intelligence Community have the capability to collect and provide economic intelligence to U.S. corporations to improve or sustain their competitiveness in the global market?

To answer this question, several supporting questions require attention. They include: What collection and analytical assets does the Intelligence Community (IC) have to provide economic intelligence? Does the IC already report on economic-related issues? If it does, what reports are available and on what economic-related topics? Are there other government agencies that provide economic information relevant to the promotion of industry competitiveness? What role do foreign governments play, in assisting their companies with the acquisition of economic intelligence?

Background

Many business leaders and individuals within the United States Government (USG) (to include some Congressmen) believe U.S. corporations have lost ground in the international marketplace. This perceived decline is attributed to the 1989 to 1993 recession and aggressive foreign technology

development and marketing. Specific concerns center on the over-all economic vitality of the United States and U.S. preeminence in the research, design, manufacturing, and marketing of key high-technology areas.

A look at some indicators of industrial health indicates the source of business and government's concern. Patent data are one index that can be used to show the technical strength of nations. From 1978 to 1988, the percentage of patents granted in the United States to U.S. inventors dropped from 62.4 to 52. In turn, the Japanese share nearly doubled from 10.5 to 20.7 percent. Japan's gains came in high-technology products, specifically computers, communications equipment, and electronic components.[4] Europe's share of patents remained approximately the same during this period, 18 percent. Figure 1 shows the national share of patents granted in the United States, by country of the patent originator.

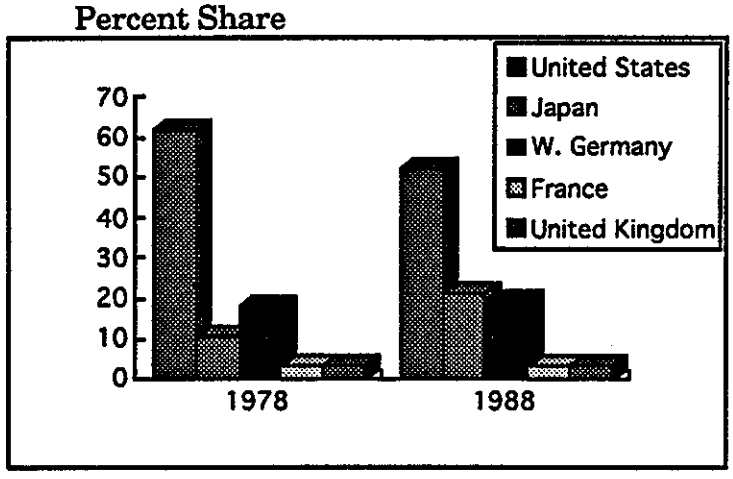

Fig. 1. National shares of patents granted in the United States, by country of origin.

Source: National Science Board, Science & Engineering Indicators-1989 (Washington, D.C.: U.S. Government Printing Office, 1989), 362.

As a result of competitor's gains, the United States' technological lead diminished in several areas. For example, the U.S. share of the world machine tool market fell from 50 to 10 percent.[5] Also, in the 1960s and 1970s America dominated the world market in integrated circuits. By 1988, Japan held 85 percent of the market share; America's share dwindled to its current eight percent.[6]

For most of the twentieth century, the United States dominated the consumer electronics industry. American scientists invented the phonograph (1887), the cathode ray tube (1897), wireless transmission of radio signals (1900), radio broadcasting (1920), television receivers (1923), magnetic wire recorders (1946), the transistor (1947), color television (1954), portable radios (1954), and home videocassette recorders (1963). Until 1970, America controlled the U.S. electronics manufacturing market it had created. But the U.S. market share is now less than five percent; Japan and Korea have taken over.[7]

America's market share for other high-technology fields has declined throughout the 1980s. Table 1 depicts this cumulative decline in high-technology manufacturing fields as defined by the Organization for Economic Cooperation and Development: industrial chemicals, drugs and medicines, engines and turbines, office and computing machinery, communication equipment, aerospace, and scientific equipment.[8]

As the table shows, other countries experienced a decline in market share also. But U.S. industry, accustomed to commanding 40 percent of the market share, perceived the 4.5 percent loss as significant; only the EC-12 lost more ground than the United States, the United Kingdom posted modest gains, and Japan's share jumped over 10 percent.

TABLE 1

MARKET SHARE PERCENTAGE FOR HIGH-TECH MANUFACTURES

High-Tech Manufacture	1980	1983	1986	1990
United States	40.4	37.8	36.9	35.9
Japan	18.4	21.6	23.4	29.2
W. Germany	11.8	11.8	11.5	9.4
France	6.2	5.8	5.2	4.7
United Kingdom	8.1	8.0	8.1	8.5
Rest-of-World	15.1	15.0	14.9	12.3
EC-12	38.5	38.0	37.1	31.4

Source: National Science Board, Science & Engineering Indicators-1991 (Washington D.C.: U.S. Government Printing Office, 1991), 402.

Note: EC-12 is the European Community. Its members are Belgium, France, Denmark, Germany, Greece, Ireland, Italy, Luxembourg, Netherlands, Portugal, Spain, and United Kingdom. The percentages for France, Germany, and the United Kingdom are incorporated into the EC-12 share.

America's mounting trade deficit has also been cause for concern for the government and industry. In American National Security: Policy and Process, former government officials Amos A. Jordan, William J. Taylor, Jr., and Lawrence J. Korb summarized the problem:

> In much of the past decade, an economic issue of great concern to national security was the mounting U.S. trade deficit, which during the 1980s had exceeded $160 billion per year. Between 1982 and 1986 the United States had grown from a net creditor nation with a surplus of over $140 billion to the world's largest debtor nation. At the end of 1991, America's cumulative net foreign debt was about $450 billion, greater than the amount owed by the next three largest debtor nations combined.[9]

The combined effect of the above listed economic indicators generated concern within business and Congress over America's world economic position.

Coupled with a concern over changing world economic status, U.S. corporations are increasingly concerned about foreign economic espionage. James Riesbeck, executive vice-president for Corning, Inc., testified before Congress that "Corning has been the target of state-sponsored industrial espionage efforts aimed at our fiber optic technology."[10] IBM's vice president for commercial and industry relations, Marshall C. Phelps, Jr., told Congress that "unfair or illegal practices by foreign competitors could jeopardize the competitive edge of the U.S. computer industry"[11] He then went on to say that IBM's losses to economic espionage have been in the billions of dollars.[12]

In 1991, the American Society for Industrial Security conducted a survey in which 37 percent of the 165 respondents reported thefts or attempted thefts of corporate secrets. "The survey revealed that the data foreign spies covet most include product development information, manufacturing technology and sales and marketing data."[13] Reported thefts or attempted thefts of commercial secrets rose from 14 percent between 1981 and 1986, to 69 percent between 1987 and 1990.[14] A short review of foreign economic espionage by U.S. allies illustrates the extent of the problem.

The Government of Israel (GOI) has spied on the United States and stolen U.S. industrial and military information for over 20 years. In 1986, operatives from Israeli Air Force intelligence tried to steal 14 boxes of corporate data from the Recon/Optical, Inc., company, located in Barrington, Illinois. The boxes contained proprietary information on the design of optics technology and advanced semiconductor microchips used in satellite

reconnaissance cameras. Data the agents removed successfully, before their arrest, went to the laboratories of the Israeli company Electro-Optics Industries. The GOI continues efforts to field a reconnaissance satellite with the services of a prime contractor--Electro-Optics Industries. [15]

Japan actively runs economic espionage operations against the United States. In the early 1980's, the companies Hitachi and Fujitsu, and the government agency the Ministry for International Trade and Industry (MITI) were caught stealing corporate secrets from IBM, Cray, and Fairchild Semiconductors. A 1987 Central Intelligence Agency (CIA) report "concluded that 80 percent of all Japanese government intelligence assets were directed toward the United States and Western Europe and concentrated on acquiring secrets about...technological developments."[16]

South Korea's equivalent of the CIA, the National Security Planning Agency, places operatives in Korean companies like Hyundai, Samsung, and the Lucky Group. The companies then post the agents to foreign countries to forge close contacts with their industrial counterparts to gather technical and financial information. One of South Korea's successes in this arena came with the placement of an agent in Washington, D.C. From the late 1960's to late 1970's, the agent made contact with corporate representatives, congressmen, senior military officers, and senior government officials. He obtained information not only on U.S. military and policy objectives but on microelectronics and petrochemicals. Reportedly, South Korea built two petrochemical complexes based on the blueprints and details provided by a cooperative American government official who did not realize he was participating in an economic espionage operation.[17]

Finally, the USG is interested in the retention of America's position as a world economy leader and its ability to maintain an over-all technological superiority over other nations. The National Security Strategy of the United States, signed by President Bush in January 1993, lists national prosperity and security as mutually supporting goals. It goes on to say:

> A top national security priority today must be to strengthen economic performance at home and economic leadership abroad. Effective participation in the global economy will be a key factor in our future prosperity and security. In 1991, U.S. foreign trade exceeded $1.2 trillion, twenty-one percent of our gross national product. The United States is the world's largest exporter of goods and services, with 1991 sales totaling $591 billion. Over seven and one-half million jobs are linked directly to our exports.[18]

The supporting National Military Strategy of the United States, lists technology superiority as vital to the national security of the United States. The importance of advanced technologies to the defensive capabilities of the nation is described as follows:

> The United States must continue to rely heavily on technological superiority to offset quantitative advantages, to minimize risk to U.S. forces, and to enhance the potential for swift, decisive termination of conflict....We must continue to maintain our qualitative edge. Therefore, advancement in and protection of technology is a national security obligation.[19]

The industrial sector that supports the military is referred to as the defense industrial base. This base, however, consists predominantly of manufacturers that also support the civilian economy. Most industries cannot afford to rely on the Department of Defense (DoD) as their principal market. "Ninety-five percent of the manufactured goods purchased by the Department of Defense come from a broad spectrum of 215 industries."[20] In 1985 DoD spent almost $165 billion on the U.S. industrial base; this

underscores how intertwined military requirements and the civilian economy have become.[21]

The technology fields supported by the industrial base and America's leaders want to protect are considered "high-technology." No single and all inclusive technologies list exists that the USG deems essential to protect. One must review official documents and extract which technologies the government considers important to national security. One document is the Militarily Critical Technologies List, or the MCTL. Compiled under the auspices of the Secretary of Defense and with industry's input, the MCTL lists and describes 15 technology categories designated critical to defense and national security (see Appendix A, Definitions, and Appendix B, Militarily Critical Technologies). The MCTL also indicates, in broad terms, the comparative technology level of other nations vice the United States (see Appendix B).

The concerns described above, a perceived (or real) decline in U.S. economic competitiveness, the economic espionage activities of foreign nations, and the USG's linkage between national security and industrial health, make the issue of economic intelligence particularly important in today's ambiguous world. As pointed out by Korb, Taylor, and Jordan in American National Security, "Political decision-makers have been answerable for traditional national security policy, but their increasing accountability for economic performance and growing economic interdependence have opened new relationships between national security and economic problems."[22]

Assumptions

The first assumption is that accurate, unclassified, information is available to conduct this study. Second, the provision of economic, or competitive, intelligence to business will continue to be a topic of interest to the current and future government administrations and to business. The USG's primary interest in economic intelligence lies with maintenance of U.S. technological parity and superiority in key high-technology fields such as the 15 listed in the Militarily Critical Technologies List.

Definitions

Two key terms used throughout this study are: economic intelligence and the U.S. Intelligence Community. These terms are defined below. The definitions for all other terms used are located in Appendix A.

There is no standard definition for the term economic intelligence. In accordance with Tyrus Hillway's Introduction to Research, the term is based on the most commonly used meanings contained in the bibliographic sources.

Economic Intelligence. Economic intelligence is analyzed and correlated information concerning the research and development (R&D), technology-level and design characteristics, manufacturing, distribution, and consumption of goods and services in the national and international economic systems. It can include details on labor, manufacturing capabilities, supporting sub-contractors and suppliers, contract bids and terms, marketing strategies, financial status and loans, customers, and policies.

A company or country may not require all these details about a competitor, but will choose to satisfy those information requirements needed

to give itself an advantage. Corporations usually use the term competitive intelligence. The USG uses the term economic intelligence, and the term economic espionage describes related foreign intelligence collection activities.

U.S. Intelligence Community (IC). The Intelligence Community is comprised of those agencies and organizations directed by Executive Order No. 12333 to conduct intelligence activities necessary for the conduct of foreign relations and the protection of the national security of the United States. The IC organizations are: the Central Intelligence Agency (CIA); the Defense Intelligence Agency (DIA); the National Security Agency (NSA); the Bureau of Intelligence and Research (INR) of the Department of State; intelligence elements of the Army, Air Force, Navy, and Marines; and the intelligence elements of the Federal Bureau of Investigation (FBI), the Department of the Treasury, and the Department of Energy.

To understand how the Intelligence Community is integrated into a true community, it helps to know that the Director of the Central Intelligence Agency is dual-hatted and also serves as the Director of Central Intelligence (DCI). The DCI is the senior intelligence official in the United States and heads the U.S. Intelligence Community. As such, he has "full responsibility for production and dissemination of national foreign intelligence" and to "establish mechanisms which translate national foreign intelligence objectives and priorities approved by the NSC [National Security Council] into specific guidance for the Intelligence Community."[23]

The DCI holds final responsibility for all USG-produced intelligence on foreign entities. As head of the Central Intelligence Agency, the Director is responsible for the operational activities of the one agency. Chapter 4,

"The U.S. Intelligence Community," explains these responsibilities in more detail.

Due to their strategic level of focus and their extensive collection and analytical capabilities, references to the Intelligence Community in this work, mean the CIA, DIA, and NSA unless other elements within the community are specified. Of note, the Central Intelligence Agency is chartered to collect, produce, and disseminate foreign intelligence and counterintelligence. The Defense Intelligence Agency collects, produces, and disseminates military and militarily-related foreign intelligence and counterintelligence. The Department of State is authorized to collect, produce, and disseminate foreign intelligence relating to U.S. foreign policy. The Department of Treasury deals with the collection, production, and dissemination of foreign financial and economic information.

Limitations

The primary limitation is that even routine government information regarding the U.S. intelligence agencies is classified. This limitation restricts the use of primary source information. The Intelligence Community does not openly discuss its capabilities, limitations, or views on the desire or appropriateness of providing economic intelligence to business. Several authors with former intelligence ties have written books and articles on the capabilities of the IC. These documents have passed classification and security reviews mandated by law before publication. In addition, public speeches from the current DCI James Woolsey, and Congressional hearing results are available. These sources will be cited often.

Delimitations

Issues that will not be addressed in this study include: national policies and laws that would need to be reviewed and possibly changed to support a decision to provide government funded intelligence to private business; and the assistance currently provided by the military services, the Defense Intelligence Agency, and the Federal Bureau of Investigation to U.S. companies, primarily DoD contractors, to improve their security to prevent technology theft and targeting of contractors by foreign economic espionage entities.

Significance of Study

Government and private industry representatives have focused predominantly on whether the United States Government "should" or "should not" provide economic intelligence to business. There appears to be an assumption that the U.S. Intelligence Community can provide economic-related intelligence and only needs Congress and the DCI to order the initiation of activities. Available sources describe the generic collection and analytical capabilities and resources of the IC but address economic intelligence capabilities vaguely, if at all. The bibliographic works have not overtly linked the should-it-be-done argument with the IC's current capabilities i.e., can it be done. This study is intended to address this basic feasibility issue, thereby providing information useful to informed discussions relating to the problem.

Summary

The recent recession, economic espionage activities by allied nations, and national security priorities have caused the United States Government and U.S. corporations to become more concerned about the global economic competitiveness of the United States. To protect U.S. economic and security interests, some industry and government officials have proposed the USG provide economic-related intelligence on foreign competitors directly to U.S. corporations. This study looks at the capabilities of the U.S. Intelligence Community to collect, analyze, and report economic intelligence.

CHAPTER 2

RESEARCH METHODOLOGY

Research Challenges

The subjects of economic intelligence and the United States Government ability to produce it are not easily studied. Confirmable information on the U.S. Intelligence Community is difficult to obtain and is not releasable, where it is classified. Private business does not openly discuss its intelligence-gathering methodologies, intelligence gains or its limitations. Industry does not openly want to reveal its own intelligence successes or failures, for fear of giving a competitor potentially exploitable information. Current public discussion on economic, or competitive, intelligence relies often on opinion, and less on quantifiable facts.

Finally, standard definitions do not exist for all the terms used in this thesis. Some terms, such as economic intelligence and economic espionage, are generally understood by business and government individuals but may be confusing to others. To facilitate thesis research and provide a common framework for discussion, definitions have been included. These combined restrictions hamper straightforward research.

Methodology Overview

Despite these challenges, a study on the U.S. Government's capabilities to conduct economic intelligence is possible. The methods used to

conduct this study include: case studies of foreign economic-related espionage; a descriptive analysis of the collection and analytical capabilities of the U.S. Intelligence Community; and a comparative analysis of the Community's capabilities as evaluated against six criteria.

Case Study

To understand the context of world-wide economic competitiveness, its importance to industry and a nation's security, and government's role in economic espionage, it is useful to study practices in other countries. American business bases itself on precepts of free-enterprise, initiative, and market-driven competitiveness. American industry's individualism takes it capitalistic character from a national tendency to resist government interference in private transactions. It can, therefore, seem strange to find that some foreign governments provide economic-related intelligence regarding competitors, American companies included, to select U.S. companies.

Case studies of the activities of two nations, France and Japan, illustrate the bond between foreign governments and business. Although several nations engage in economic espionage, as indicated in Chapter 1, France and Japan provide illustrative examples of foreign governments' actions.

It is this direct link between government and business that some individuals propose to establish between the U.S. Government and U.S. businesses. Anticipated rewards of such a relationship include: reduced product research and development (R&D) timelines, reduced R&D costs, accelerated time from R&D to product marketing, and the receipt of lucrative

contracts by undercutting a competitor using inside knowledge of his bid and terms. In sum, any benefit gained in these areas has the potential to increase profits.

The predominant sources for these studies are: Friendly Spies: How America's Allies are Using Economic Espionage to Steal Our Secrets by Peter Schweizer; Protecting America's Secrets in the Global Economy published by the American Institute for Business Research; and The Threat of Foreign Economic Espionage to U.S. Corporations, based on Congressional hearings held by the House Subcommittee on Economic and Commercial Law.

Descriptive Analysis

After reviewing the actions of two other countries' intelligence communities, the next step will be to review the capabilities of the U.S. Intelligence Community. The first step in this description will be to outline the collection methods, or types of intelligence, used by the IC. These intelligence fields make-up the collection capabilities of the Community. The intelligence collection methods are: human intelligence (HUMINT), communications intelligence (COMINT), imagery intelligence (IMINT) and open source intelligence (OSINT). Each " INT" brings unique capabilities to the IC and provides a basis for which any intelligence activity, to include economic intelligence, can be conducted. Therefore their strengths and limitations will be evaluated in relation to the economic intelligence issue. These terms are defined in Appendix A.

The next description will include an overview of agencies that collect and analyze foreign intelligence and might, therefore, have the potential to collect foreign economic intelligence. This overview will consist of assigned

collection and reporting functions and the strengths and limitations of each agency, particularly the potential to report economic-related intelligence.

The agencies are: the Central Intelligence Agency (CIA), the Defense Intelligence Agency (DIA), the National Security Agency (NSA), the Department of State, and the Department of Treasury. As will be explained later, the intelligence components of the military services feed their information to DIA and so will not be considered separately.

Other elements of the USG have defined economic-related reporting responsibilities although they are not members of the IC. Since their information could theoretically be blended into that of the IC, these agencies will be considered for their capabilities also. These entities include: the Department of Commerce and the Office of the Under Secretary of Defense for Acquisitions (International Policy)(USDA(IP)).

The major sources contributing to this analysis are: Deep Black by William Burrows; The U.S. Intelligence Community: Foreign Policy and Domestic Activities by Lyman Kirkpatrick; Jeffrey Richelson's The U.S. Intelligence Community; and Silent Warfare: Understanding the World of Intelligence by Abram Shulsky.

Comparative Analysis

The final step will be to compare the combined strengths and limitations of the IC and other designated elements within the USG against intelligence reporting criteria. As mentioned earlier, it is difficult to assess the Intelligence Community's effectiveness due to its operating secrecy, collection method and product classification, and characteristics of its

customers. Despite these hindrances, some inferences can be drawn from available information and discussion regarding the IC.

With this information, the capabilities of the IC will be evaluated against the following criteria:

Accuracy. Can the IC provide accurate information usable by business? Would the IC's intelligence be more accurate than commercially-generated intelligence?

Cost. Can the cost of obtaining economic intelligence be calculated? Would taxpayers, interested companies, or both pay for the information? Are the IC's assets capable of responding to increased responsibilities, or would mission trade-offs occur?

Releasability. Can the IC provide usable unclassified information to business or will desirable information remain in intelligence channels due to release restrictions applicable to classified information?

Suitability. Can the IC provide the appropriate type of information desired by business, such as: R&D program details; component and material design, composition, and manufacturing capabilities; and contract and negotiation details? The Intelligence Community can provide information on GNP and per capita income of a nation but generic economic information is available from other sources, such as the Department of Commerce, and is marginally useful to individual corporations.

Target Accessibility. Can the IC obtain access to the target to get the desired information? How readily and at what risk? Can the IC/USG provide economic-related intelligence that business cannot obtain on its own?

Timeliness. Can the IC provide timely information to business in time for it to be used effectively by management? Some economic and business aspects might not be critically time sensitive; however, knowledge about a competitor's contract bid and terms might give the information recipient the chance to submit a lower bid or provide more favorable terms in order to gain the contract.

Summary

Complete information on the Intelligence Community is difficult to obtain. Publicly available information may not as complete as one would like and some commonly used terms have not been defined. To conduct this study, sources have been used that include Congressional documents, books from former government officials, and interviews and speeches from senior USG intelligence officials. Some terms, such as economic intelligence, have been defined. Challenges notwithstanding, materials used for this study will be evaluated through case studies of foreign espionage activities and descriptive and comparative analyses.

CHAPTER 3

FOREIGN GOVERNMENTS' ROLE IN ECONOMIC ESPIONAGE

Overview

Foreign governments conduct economic espionage for the reasons described in Chapter Two: to shorten R&D times, reduce R&D costs, accelerate products to market, and preempt contracts from competitors. While testifying before a Congressional committee, DCI Robert Gates (1991-1993) described the economic and business information targeted by foreign governments to help them achieve the above aims: U.S. Government policies on foreign trade, investments, loans, positions on bilateral economic negotiations; and contract bids, commodity pricing, financial data, and banking information on stock market trends and interest rates.[1]

The House of Representatives Subcommittee on Economic and Commercial Law held hearings on foreign economic espionage activities conducted against U.S. corporations in spring 1992. During his testimony, DCI Gates gave an overview of six collection patterns used by other countries to gain the desired information.[2]

Pattern one consists of classic espionage. A foreign intelligence organization clandestinely recruits and manages paid agents in U.S. companies and government organizations. Agents may be U.S. citizens or foreign employees of a U.S. corporation. In the second pattern, the foreign organization relies on the elicitation of information. This type of collection

activity is low-key and often not obvious to the target. The agent is likely to ask openly for information such as marketing statistics, an organizational roster with telephone numbers, or the status of an on-going R&D project. Commonly, the agent plays on the sympathy of the target as a business friend or the shared interests between his country and the United States.

Third, the intelligence organization operates within its own country, searching the hotel rooms of visiting American officials and businessmen for business data and planting listening devices in them. Items searched include luggage, briefcases, and the electronic files on laptop computers. In some instances, the items may be stolen outright.

Fourth, the foreign government collects economic or business information from non-intelligence, predominantly open, sources. Open source intelligence comes from public tax returns, company reports to stockholders, business and trade magazines, on-line computer databases -- any publicly available information source. Fifth, a government uses front organizations, military attaches, and covert (spy) intelligence units to target scientific and technical technologies and information in a foreign country.

In the last pattern, private entrepreneurs sell their collection and analytical services to governments or corporations. The commercial field of competitive intelligence (CI) continues to grow with the formation of consultant companies that specialize in either collecting and providing information to other firms or teaching them how to form their own CI sections. Such consultant companies include Washington Researchers and Washington Information Group Ltd. Competitive intelligence researchers and companies stress that their methods are legal; their information comes from open sources.

According to Robert Gates, approximately 20 countries engage in intelligence activities detrimental to U.S. economic interests.[3] U.S. corporations and the USG do not like to discuss details of economic espionage by foreign intelligence services. Government's sensitivities arise from the sponsorship of economic spying by U.S. allies. Political and military alliances that are otherwise cooperative in nature can be damaged by accusations of espionage. In turn, corporate reluctance to discuss its victimization derives from the harm disclosures cause to a company's business.[4] Negative publicity can result in a drop in the company's stock prices, lowered company morale, the pull-out by corporate partners for fear of losing their secrets, and the loss of contracts in the accused country.[5]

Despite official reticence to discuss foreign-sponsored economic spying activities, some instances have become public. To understand the depth of the problem and U.S. industry's concerns, some publicized activities by France and Japan will be discussed, although many other countries also engage in economic espionage.

Case Study: France

France has conducted economic espionage against the United States for 30 years and is quite honest about its activities.[6] Pierre Marion, a former director of the Direction General de la Securite Exterieure (DGSE)(France's equivalent to the CIA), said in a September 1991 NBC interview "...getting intelligence in economic, technological, and industrial matters [from] a country [with] which you are allied...is not incompatible with the fact of being allied."[7] In the same interview, he continued, "It would not be normal that we do spy on the States in political matters or military matters, but in the

economic competition, in the technological competition, we are competitors; we are not allied."[8] As will be described through examples, the DGSE's collection methods include covert procedures that consist of: recruitment of agents within a corporation, theft of information or materials, and electronic eavesdropping.

The DGSE plants microphones near first and business-class seats on Air France flights from the United States to Paris to listen to business conversations.[9] The French intelligence agency also places monitoring devices, or bugs, in the hotel rooms of foreign business executives in Paris. Agents sometimes enter the rooms of visiting businessmen to either view or steal the contents of briefcases and laptop computers.[10]

In April 1990, GTE officials, while in France, found important company papers missing from their briefcases. Later that year, AT&T representatives experienced the same type incident. In early 1991, executives from NCR had laptop computers stolen from two rooms.[11] The computers contained electronic files of proprietary company information. DGSE involvement cannot be proven but this type of activity is consistent with its acknowledged behavior.

In a specific case that began in 1987, DGSE officials identified three U.S. companies whose proprietary information could benefit France. France targeted IBM and Texas Instruments as computer industry leaders, and Corning for its fiber optics knowledge and capabilities. In a few months, senior American officials were recruited in the French offices of each company. At IBM, the recruited individuals had access to senior business decisions, financial information, contract bids, research information, and sales. DGSE funneled the information to the French electronics firm

Compagnie des Machines Bull. The French government felt that the Bull company needed the knowledge to keep it from lagging further behind foreign competition in R&D, production, and marketing. The entire operation ended after a DGSE agent with a drinking problem became too talkative. In 1989, the CIA and the FBI broke up the network. In private, DGSE admitted its involvement to the CIA.[12] The names of the American corporate recruits have not been released.

IBM is a world leader in computer hardware, software, and system integration development. Marshall Phelps, Jr., an IBM vice president, maintains that U.S. industry has more than 60 percent of the world market in sales of computer software, accounting for over $63 billion annually.[13] IBM owns a large part of the 60 percent share; France would likely welcome a share of such a market.

The industrial importance of Corning, Inc. to industry derives from its world preeminence in specialized glass manufacturing. Corning, headquarted in upstate New York, invented the process for making glass blanks for the first electric light bulbs and glass for televisions. It developed the ceramic core of the catalytic converter, silicone, photochromic lenses, and specialty ceramics used in space exploration. Perhaps most importantly, Corning invented the process for making and remains the world's leading manufacturer of fiber optics.[14] Fiber optic cables are used primarily in communications. James Riesback, executive vice-president for Corning, testified before Congress in 1992. He stated that Corning has been the target of state-sponsored economic espionage but did not elaborate.[15]

In a less sophisticated operation in 1992, French engineers came to the United States to collect technology information. DGSE provided the

French engineers a list of U.S. chemical firms that produced stealth aircraft coatings. Once they were in the United States, the engineers called company scientists. They openly asked the American workers to give them the classified formulas and processes used in stealth technology. Their rationale for this request centered on the allied relationship between the United States and France. The engineers argued that both countries would benefit from the one-way exchange. This was a classic case of elicitation. One American scientist contacted the FBI who in turn notified the companies that they were espionage targets.[16]

More recently, a DGSE document, leaked to the USG and the U.S. media in 1993, listed over 35 U.S. corporations and banks targeted by the French government for economic espionage. Its contents, depicted in Table 2, indicate France wants information on "computers, electronics, telecommunications, aeronautics, armaments, nuclear, chemical, space, consumer goods, capital goods, raw materials, and major civilian contracts."[17]

French successes in these collection operations cannot be determined. American companies and agencies, such as the 35 listed below, understand they are targets and presumably take security actions to prevent obvious thefts from foreign spies. However, one can infer French actions reap profits from two facts: France admits to a 30 year history of economic espionage and comments from former senior French intelligence officials hint at success.

TABLE 2

U.S. COMPANIES TARGETED BY FRENCH GOVERNMENT FOR INDUSTRIAL ESPIONAGE

Allied Signal	Los Alamos and Lawrence Livermore National Labs
Bankers Trust	LTV
Bell	McDonnell Douglas
B.F. Goodrich	Martin Marietta
Boeing	Merrill Lynch
Chase Manhattan Bank	Morgan Guaranty
Chemical Bank	Motorola
Corning Glass	NASA Space Centers
First Boston Bank	Northrop
Ford Aerospace	Pratt and Whitney
General Dynamics	Prudential Bache
Goldman Sachs	Rockwell International
Grumman Aerospace	Soloman Brothers
GTE	Texas Instruments
Honeywell	TRW
Hughes Aircraft	United Technologies
Lockheed	Westinghouse

Source: Bill Gertz, "French Probed as Spies Against U.S. Companies." Washington Times, 4 June 1993.

Like Pierre Marion, another former spy master, Count Alexandre de Marenches headed the forerunner to the DGSE from 1970 to 1981. In his 1986 memoir, Dans le Secrets des Princes, de Marenches wrote, "In any Intelligence Service worthy of the name one would easily find cases where a single operation [involving the economy, industry, and science] paid the year's operating budget. Naturally, the Intelligence Service does not receive [direct] remuneration but the country's industry profits."[18]

The Fourth World War, another book by de Marenches, contains additional revelations about the importance of economic espionage to France.

The DGSE's Director of the Economic Intelligence Service told de Marenches that the United States was going to devalue the dollar on 18 December 1981; he also knew the devaluation amount. President Pompidou had the Banque de France, the equivalent of the United States' Federal Reserve, take advantage of this financial information. Working through contacts whose association with the French government could be denied, the Banque sold dollars and bought francs in markets around the world, accumulating enormous profits.[19]

De Marenches does not relate how France collected the information nor the profit achieved. He provides hints that the sum totaled in the millions of dollars. "Were we not profiting from the misfortunes of a friend and ally? Perhaps. But at times, ...that's part of the game."[20]

In a second acknowledged incident, France sold $1 billion worth of Mirage jet fighters to India, in 1981, beating competition from the United States and the Soviet Union. To quote Marion again, "We were able to get the contract mainly because we did get some inside information about the proposals which had been made by the other two competitors."[21] Given their history of economic and industrial espionage, France will presumably continue to conduct these intelligence operations.

Case Study: Japan

While former intelligence officials Alexandre de Marenches and Pierre Marion have provided candid insights on French economic espionage activities, Japanese officials have not been so open. Available information comes predominantly from former USG officials who have openly discussed

Japanese activities. From their comments, one can conclude that Japan actively seeks economic intelligence from any high-technology competitor.

Much as the United States links technological superiority and economic vitality with national security, so too does Japan. Indications exist that Japanese businessmen are aware that technological and economic preeminence grant the holder a great deal of power. Sony Corporation's chairman, Akio Morita, and Diet (parliament) member, Shintaro Ishihara co-authored a book, A Japan That Can Say No. Released in 1989, the author's maintain that "Japan can change the whole world balance of power."[22] Ballistic missiles cannot be targeted without the use of Japanese semiconductors, per their example, and Japan could shift world power by deciding which country to sell and which country to deny its semiconductors.[23]

Of note, Clyde V. Prestowitz, a former Department of Commerce official notes that A Japan That Can Say No is unpublished in English. Sony declines requests to provide copies of the document. "Reports from Tokyo say the book is intended only for a Japanese audience."[24]

Japan operates its economic collection bureaucracy in a manner different from France. The Japanese government itself does not provide large amounts of intelligence to its corporations. Companies maintain their own extensive intelligence gathering assets. Instead, the Japanese government provides direction and money; it also collates the information provided to it by companies.

Government agencies, the Ministry for International Trade and Industry (MITI) and the Japanese External Trade Organization (JETRO), coordinate national economic collection priorities, provide access to foreign

countries (through trade offices), and channel the intelligence they do collect to the appropriate industry. JETRO operates 77 offices in 59 countries; its agents collect economic and technical information and forward it to MITI.[25] According to Japan: 2000, a report commissioned by the CIA, "Japan's elaborate system for political and economic intelligence is conducted through the various trading companies down to the office level."[26]

A 1987 classified CIA report, Japan: Foreign Intelligence and Security Services, reported that Japan's national intelligence priorities were:

1. Intelligence on technological and scientific developments in the United States and Western Europe.

2. Intelligence on political decision-making in the United States and Europe relating to trade, monetary, and military policy in Asia and the Pacific region.

3. Intelligence regarding access to foreign sources of raw materials to include oil and food.

"The report concluded that 80 percent of all Japanese-government intelligence assets were directed toward the United States and Western Europe and concentrated on acquiring secrets about and information on technological developments."[27]

France's Economic Espionage Experiences with Japan

In an interesting disclosure twist, the French former intelligence official, Alexandre de Marenches describes the Japanese as experts in economic espionage. He relates that the Japanese government and industry have close ties with each other. The French intelligence agency, DGSE, studies Japanese intelligence operations abroad, trying to determine Japan's

next technology target. According to de Marenches, Japan examines the global production situation, determines which country can satisfy their high-technology requirement, and then dispatches a collection delegation.[28]

In late 1978, the British government intercepted telephone conversations of detailed Japanese plans to acquire illegally a French digital telephone switching system. The British government notified France, an act that reveals the extent of intelligence exchanges between some nations. When contacted on the matter, the French telecommunications company expressed astonishment; it thought the Japanese were interested in buying not stealing the technology.[29]

The DGSE mounted an intelligence collection effort to discern Japan's plan. Through simple techniques, members of the Japanese negotiating team toured the French plant, spoke with design engineers, and took photographs of equipment and manufacturing processes. While listening to conversations in the team's hotel room [via electronic eavesdropping equipment discussed earlier], French intelligence heard the Japanese exchange information, analyze the photographs, and assign collection requirements for the next day. One delegate was to get a French designer to discuss the switching system in detail; another was to take more detailed photographs of plant equipment.[30]

Alerted by the DGSE, the French company refused to grant the Japanese further access to manufacturing details. Abruptly, Japan canceled the remainder of the visit and broke off contract talks.[31]

Japan apparently gathers industrial information through other surprisingly simple means. Although he provides no examples, de Marenches claims that Western companies, eager to obtain Japanese contracts, have

sent [unspecified] product samples to Japan for review. Months later, according to de Marenches, the item can be found on sale in Western markets, with "Made in Japan" stamped on it.[32] One can assume this has happened to French companies otherwise de Marenches would likely not have mentioned it.

How the Japanese obtain information or who provides it to them in some cases is never discovered. At one time, the French secret service covertly and regularly opened the diplomatic pouches of foreign embassies based in Paris. (A telling incident in itself about French espionage activities.) In 1974, it found information on the French optics industry, including confidential memos from two French companies, in the Japanese embassy pouch. France let the documents go as it did not wish to disclose its own espionage activities.[33]

The American Experience

During Congressional hearings, former DCI Gates stated that "the principal characteristics of the Japanese competitive intelligence effort is its massiveness, including a very large scale, comprehensive, overt collection and analysis activity."[34] One overt and legal means to acquire technology is through co-production agreements. Japan initiated such an effort through the FSX fighter. The FSX fighter is a fighter aircraft the Government of Japan wanted developed to meet Japan's defense needs.

Clyde V. Prestowitz, Jr., served as the Counselor for Japan Affairs to the Secretary of Commerce from 1983 to 1986. During his tenure, the USG and Japan negotiated co-production of a fighter aircraft, the FSX, for the Japanese Defense Agency. The entire FSX issue was politically contentious

for both countries. Japan claimed it needed a specially designed fighter that would require technical assistance from the United States to build. The USG maintained that the F-16 aircraft could fill Japan's defense requirement and do it for less money. Japan insisted on access to U.S. technology under a co-production agreement to design and build the unique FSX.[35]

Co-production agreements can be beneficial to all involved parties. Sometimes they are not. Problems with co-production arrangements can occur when one partner gains considerably more from the deal, through jobs, profits, or technology, than the other contributors. Additional complications arise when the gaining partner acquires proprietary information or technology it may sell or trade to other countries without permission of the originator. USG and aircraft industry officials held all these concerns about the FSX deal.[36]

During the FSX negotiations, Prestowitz routinely read intelligence reports from the CIA concerning the issue. The CIA continuously provided details of Japan's political and negotiating positions and true reasons for wanting to develop a new fighter vice purchase of an off-the-shelf aircraft.[37]

One agency study "concluded that the FSX deal would significantly enhance Japan's ability to develop military aircraft on its own and to become an important competitor of U.S. industry in commercial aircraft."[38] The U.S. and its contractors would gain little in jobs, money, and technology; Japan would reap significant rewards. "Japan hoped to obtain U.S. technology with regard to design and development, systems integration, composite materials, and engines."[39] Analysts judged that Japan was ten years behind U.S. manufacturers in sophisticated aircraft construction techniques, composite materials, phased-array radars, and software source codes.[40]

Open-source material, available during this time period, reinforces the CIA's analysis. A Japanese magazine article,

> said that Japan's objective was to become a world-class aerospace competitor, a position it planned to achieve by learning [about related technologies] through co-development arrangements: "Those in the United States who oppose transferring technology to Japan pierced through to the true root of Japanese intentions."[41]

FSX negotiations between both governments lasted almost seven years. Individuals in Congress, the Department of Defense, and business continued to express concerns about the implications of high-technology transfers to Japan. Finally, in 1989, President Bush reached an agreement for the U.S. to get 40 percent of the production of 120 fighters. Japan would receive 60 percent of the production, valued at approximately $6 billion dollars, along with the acquisition of U.S. technology needed to design and build the fighter.[42] In the end, President Bush agreed to the deal to support the U.S. fighter industry (40 percent of production appeared better than none) and erase 5 percent of the trade deficit with Japan.[43]

Clyde Prestowitz and 35 then (1989) members of Congress, including Senators Alan Dixon (D, IL), Robert C. Byrd (D, WV), Lloyd Bentsen (D, TX), and Alfonse D'Amato (R, NY), maintained reservations about the one-sided FSX deal and the transfer of technology to Japan. Concerns included the possibility that U.S. technology passed to Japan will eventually be incorporated into Japanese products sold to compete against U.S. products.[44] Despite significant opposition to the agreement, the Senate failed to halt the FSX deal, falling one vote short.[45]

Senate concerns over Japanese take-overs in some industries are based on past activities. Japan has already succeeded in taking over what had been one U.S. dominated industry. In 1972, Japan targeted the U.S.

microchip industry for economic-related espionage. The Japanese Diet (parliament) directed the establishment of an intelligence-gathering effort. MITI had oversight responsibility for the entire program. "A Committee on Information and Acquisitions was set up...to direct the acquisition of foreign intelligence on [microelectronic] technological developments in the United States."[46]

The committee coordinated collection activities with JETRO and five Japanese electronics companies with representatives in the United States: Hitachi, Fujitsu, Mitsubishi, NEC, and Toshiba. Collection efforts centered on Silicon Valley in California. Japanese espionage efforts were aggressive; the Central Intelligence Agency and Federal Bureau of Investigations recognized what was happening. In 1980, the State Department began to reduce the number of visas granted to Japanese businessmen traveling to the U.S. to work in Japanese companies.

Japan succeeded in its efforts and achieved a significant pay-off. CIA analysts estimated that Japan's intelligence operations provided as much as 70 percent of the base-line date needed to manufacture specialized microchips.[47] The results of this effort are almost staggering.

> By 1980 Japanese companies had surpassed U.S. merchant semiconductor firms in the design and manufacture of the latest generation of semiconductor devices. By 1983 Japanese-based firms held a share of the world market equal to that of U.S.-based firms. By 1986 the Japanese had taken 65 percent of the world market for memory products, while the U.S. share had fallen to 30 percent. In 1988 Japan held 85 percent of the market for one megabit memory chips, while the American share...had dwindled to eight percent.[48]

Japan's espionage techniques resemble those of France at times. Hotel rooms in Japan are bugged and searched. One U.S. businessman, who traveled to Tokyo in 1990, relates that someone went through business

papers in his hotel room. He discovered this by accident; pages in his documents had been restapled upside-down. When he questioned hotel officials about such activities, they shrugged and told him that if anything had been done, it was done legally.[49]

Japan also hires consultants in foreign countries to help Japan negotiate local laws and lobby foreign governments and businesses on its behalf. By the early 1980s, U.S. consultants for Japan included former DCI William Colby, Richard Allen, a former national security advisor to President Reagan, and Frank Weil, former Assistant Secretary of Commerce.[50]

Indications exist that consultants provide intelligence in addition to advice. "In March 1984, the Gartner Group, a prestigious consulting firm, settled with IBM out of court over allegations that the firm had sold confidential memos to IBM's Japanese competitors."[51] In Chapter 5, another such incident is related where a U.S. consulting firm passed information received from a senior intelligence official to a Japanese company. The company in turn sent the information to the Japanese government.

Analysis of Foreign Activities

France's and Japan's economic espionage activities share common points. In these countries, economic espionage is:

1. Government sponsored.
2. Deemed important to national security.
3. Keyed to national-level economic goals and desired high-level technologies.
4. Its results are passed to private or state-owned industries specializing in the technology or related manufactured goods.

5. Its conduct indicates the government has the will, and more importantly, the capabilities within its national intelligence services to collect the targeted information; its analysis is conducted by either the government or the company which receives the information or technology.

6. The information can, in some instances, be collected and used in a timely manner to the benefit of the country and its companies.

Such activities are not limited to France and Japan. Examples exist where other countries, to include South Korea and Israel, engage in economic espionage. One can project that only a limited number of economic espionage incidents ever come to public attention. The extent of economic intelligence activities cannot be estimated; however, the number of incidents presented here and comments made by various officials indicate a great deal of international activity occurs constantly.

Summary

Foreign countries, some of them U.S. allies, conduct economic espionage against the United States. Specifically, candid disclosures from U.S. and foreign officials reveal that France and Japan have run economic espionage activities against the United States for at least 30 years. These, and other countries, target select high-technology, financial, and related policy decisions for acquisition. Espionage efforts are coordinated by the foreign governments and executed by intelligence organizations or business proxies. Collection activities are aggressive and occur in the parent country and overseas. Information obtained through espionage can benefit the gaining country immensely through reduced R&D time and costs, increased profits, and improved market competitiveness.

CHAPTER 4

THE U.S. INTELLIGENCE COMMUNITY

Overview

The Intelligence Community (IC) elements with economic intelligence collection and reporting responsibilities are the Central Intelligence Agency (CIA), the National Security Agency (NSA), the Defense Intelligence Agency (DIA), the Bureau of Intelligence and Research (INR)(Department of State), and the Office of Intelligence Support (Department of Treasury). Additional entities, not part of the IC, with economic-related reporting responsibilities include the Department of Commerce and the Under Secretary of Defense for Acquisition (International Programs)(USDA/IP)(Department of Defense). These are the primary government agencies with economic intelligence responsibilities.

The head of the CIA, a civilian presidential appointee, holds two responsibilities: Director of the Central Intelligence Agency and Director of Central Intelligence (DCI). As head of the CIA, the director is responsible for activities of the one agency. CIA's deputy director runs day-to-day matters as the director is more involved with his second job as DCI. The President's appointee as DCI is the senior intelligence official in the United States. The other heads of the agencies within the Intelligence Community report to him. In turn the DCI, currently James Woolsey, reports directly to the President for all USG intelligence matters. Some individuals confuse the roles of the

Director of the CIA and Director of Central Intelligence and use the terms interchangeably. However, both jobs have separate and distinct responsibilities as indicated above.

The directors of the National Security Agency and the Defense Intelligence Agency are senior military officers (three star rank). The Department of Defense nominates individuals to fill these positions, and Congress confirms the nominees. Both directors hold military intelligence support responsibilities to the Secretary of the Defense and the Joint Chiefs of Staff. In the execution of their intelligence collection and reporting jobs, they follow executive orders, federal law, and guidance from the Director of Central Intelligence. Figure 2 depicts the major components of the Intelligence Community discussed in this thesis.

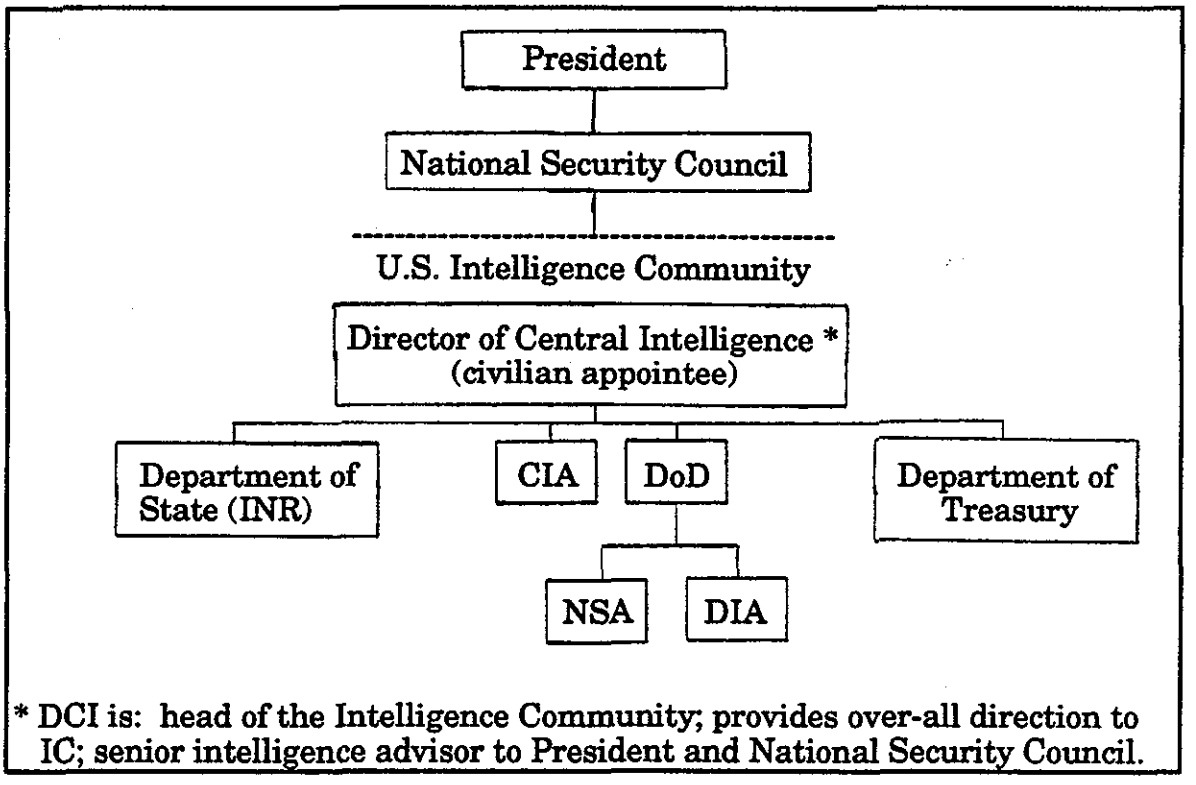

Fig. 2. U.S. Intelligence Community.

Source: Adapted from Ames. A Jordan, Lawrence J. Korb, and William J. Taylor, American National Security: Policy and Process (Baltimore and London: The Johns Hopkins University Press, 1993), 145.

Intelligence Functions

The members of the Intelligence Community, and those agencies with adjunct intelligence roles, perform a variety of assigned intelligence collection, analysis, and reporting responsibilities. The USG definition of intelligence is located in Appendix A. A working definition derived from the official one is: intelligence is the product that results from the collection, evaluation, and analysis of information. Products range from memorandums to studies, books, briefings, charts, videotape, and recordings. The term

"intelligence information" indicates raw and unevaluated material from any source and any medium which relates to the topic of interest.

Several sub-categories of intelligence exist which relate to collection means. Commonly referred to intelligence categories include: communications intelligence (COMINT); human intelligence (HUMINT); imagery intelligence (IMINT); and open source intelligence (OSINT). These terms are located in Appendix A, but abbreviated definitions are included here.

Communications intelligence (COMINT). Information extracted from the interception and analysis of electronic and voice communications. Specific types of intercepted communications are discussed below, in the section dealing with the National Security Agency.

Human intelligence (HUMINT). Intelligence derived from the collection and analysis of information obtained by human sources.

Imagery intelligence (IMINT). Information derived from the collection and analysis of any medium capable of producing an image. Images include photographs and electronic displays.

Open source intelligence (OSINT). Information taken from sources available to the general public. There are no limits on the medium or source involved. As an example, this thesis was written from "open source" information: books, magazine and newspaper articles, government documents, published interviews, and a televised speech.

The intelligence agencies and government entities described here analyze information from these collection methods. Collectively, this is known as "all-source" analysis. Unevaluated information, or "raw" reports from collectors are shared between agencies to varying degrees. Analysts

within the agencies review, evaluate, analyze, interpret, and compile the information into completed, or "finished," intelligence products. What differs between agencies is their reporting and operation of collection assets responsibilities.

"The results of their efforts--intelligence products--range from nearly real-time [immediate] current intelligence reports to longer-term, forward-looking reports which are fully coordinated by all concerned agencies at the national level."[1] Intelligence consumers, or customers, include the national leadership (such as the President, National Security Council, Congress) and their advisors, and analysts who are members of the Intelligence Community.

Intelligence Agencies

Central Intelligence Agency

The National Security Act of 1947 established the CIA. Its basic charter, outlined in Executive Order 12333, is to collect, produce, and disseminate foreign intelligence. The term "foreign intelligence" is all encompassing and includes economic-related intelligence by default.

The Central Intelligence Agency is the oldest and most senior of the intelligence agencies. It has up to 20,000 employees and a budget of approximately $3.2 billion.[2] Its personnel publish intelligence products on subjects that include but are not limited to foreign governments, militaries, and weapons systems; narcotics production and trafficking; and terrorism. CIA's reporting variety can be seen in the following titles: "Nicaragua: The Outlook for the Insurgency" (1983); "The Cuban Foreign Policy" (1979); "Terrorist Use of Chemical and Biological Warfare" (1985); and "Iran: Prospects for Near Term Instability" (1985).[3]

The Directorate of Operations manages clandestine collection activities, more commonly referred to as "spy" operations. Within the Directorate, one division conducts oversees clandestine activities: recruiting, obtaining information from, and paying spies in foreign countries. A separate element, the National Collection Division, openly collects information from U.S. citizens who travel abroad such as scientists, engineers, economists, academicians, and energy experts. These individuals provide information gained at international conferences, fairs, workshops, and foreign trade meetings.[4] Both the classic spy activities and assistance provided openly from U.S. travelers abroad are HUMINT operations.

The agency employs economists who "monitor such trends as the annual Soviet [now Russian] wheat harvest, Chinese industrial output and Middle Eastern oil production."[5] Secrecy notwithstanding, former DCI Robert Gates conceded, in an August 1993 interview, that approximately "40 percent of intelligence that's routinely gathered [by the CIA] is economic in nature."[6] Amounts and types of information collected, analyzed, processed into intelligence and disseminated are otherwise not available.

Discussing CIA's activities in a speech aired on television in November 1993, DCI James Woolsey stated that the Central Intelligence Agency was not going to be in the business of providing economic intelligence to U.S. companies in the manner of allies [who provide intelligence to their own companies]. He emphasized that the agency would continue to provide the following economic-related intelligence to government decision makers:

1. Trends in global and individual countries' economic policies;

2. How well or how poorly East Europe and the Former Soviet Union are doing in economic development;

3. Assess how some governments violate the "rules of the game" by using their intelligence services for industrial espionage against U.S. companies to seek an unfair advantage and using pressure to help their own firms obtain contracts they would not otherwise get through fair trade.[7] Key to this speech is Woolsey's confirmation the CIA can report on foreign economic policies, developments, foreign government espionage activities, and details on foreign individual companies that benefit from government espionage.

Defense Intelligence Agency

The Defense Intelligence Agency (DIA) reports to the Secretary of Defense via the Joint Chiefs of Staff. DIA has several responsibilities; its basic ones are: provide foreign military-related intelligence to the Secretary of Defense and DoD components; coordinate all DoD (military) intelligence collection and production requirements; and manage the Defense Attaché System (DAS).[8]

DIA differs from CIA in that it produces intelligence on foreign military matters. CIA produces intelligence on foreign civilian and military matters. Specifically, DIA reports on the size and composition of foreign armies, air forces, and navies; foreign military weapons--missiles, fighter and bomber aircraft, tanks--their numbers within a foreign military and their capabilities.

Some overlap exists within these responsibilities. Executive Order 12333, which outlines the responsibilities of the Intelligence Community, directs the DCI to ensure that "appropriate mechanisms for competitive analysis are developed so that diverse points of view are considered fully and

differences of judgment within the Intelligence Community are brought to the attention of policy makers."[9] The DCI and the Secretary of Defense are charged to ensure that there is no "unnecessary" overlap between the various agencies' intelligence programs.

Since its mission is military in nature, the Defense Intelligence Agency does not report on core economic intelligence subjects, such as trade negotiations, national GNP or trade deficit figures, or contract details and bids. The CIA does instead.

DIA contributes to a sub-element of economic intelligence. It brings to the Intelligence Community a strong Scientific and Technical Intelligence (S&TI) analysis and reporting ability. S&TI incorporates the research and development, production, and marketing of military and dual-use technologies.[10] Dual-use technologies have both military and civilian applications; satellite imagery systems, nuclear power plant designs and equipment, Global Positioning Satellite (GPS) equipment, advanced generation night vision devices, and cellular communication systems are some examples.[11]

DIA employs scientists, engineers, and other analysts with technical backgrounds to assess the scientific and technical level of targeted countries. In effect, DIA has a responsibility to track and understand worldwide technology capabilities and assess the quality and extent of the world's industrial base.[12] Analysts provide input to the evaluation of other countries' high-technology bases; their assessments are included in the Militarily Critical Technology List documents, which will be described in more detail later. Other government entities report on or provide input to S&TI also. They include CIA, the National Laboratories, and the military services.

In April 1993, DIA officials submitted a Joint Strategy Review (JSR) paper, Joint Strategy Review Plan Key Judgment Paper: Technology Proliferation and U.S. Technological Superiority, to the J-5 (Strategic Plans and Policy) component of the Office of the Joint Chiefs of Staff. Officials presented intelligence issues that in their view require collection and analysis by the Defense Intelligence Community. These issues were selected for their impact on U.S. superiority in key militarily-related technology fields deemed important to national security: computers, software, sensors, communications networking, electronic devices, environmental effects, materials and processing, energy storage, propulsion and energy conversion, design automation, and human-system interfaces.[13]

Intelligence issues selected for desired future collection and analysis emphasis included:

1. The monitoring of foreign students in the United States, from selected countries, noting their study disciplines and research efforts.

2. World-wide monitoring of major research and development facilities to prevent technological surprise and offer DoD potential sources for advanced technologies.

3. Establishing a foreign material acquisition program to acquire and exploit weapons components and systems to assess their technological level and develop countermeasures to the system.

4. Developing a program to acquire state-of-the-art dual-use technologies and components on the world market. This effort could be a prelude to commercial component stockpiling and testing where domestic R&D and production are nonexistent or lag behind other countries' capabilities.

5. Developing more reliable co-production agreement oversight mechanisms. This relates to the unauthorized sale or transfer of U.S. technology from a country involved in co-production agreements, usually for defense systems, to an unapproved recipient nation.[14]

Through interpretation, this JSR indicates what DIA does not do in the collection and analysis of S&TI. That officials raised the issue to the Joint Chiefs of Staff indicates the importance of technology to national security and the Intelligence Community's recognition of it. The link between S&TI and economic intelligence lies in the desire to procure foreign military and dual-use technologies. JSR issues state that technology acquisition would reduce system and component R&D times. This could reduce defense costs and benefit U.S. industry through the acquisition of technologies for marketing to other countries. The JSR indicates DoD's S&TI effort is basic and not at the sophistication level deemed sufficient to support national security.

Analysts use information from all sources to make their assessments. The agency does manage one collection capability, the Defense Attaché System (DAS). Defense attaches are military personnel, from all the services, who overtly acquire military-related information. "They make no secret of the fact that they are intelligence officers, diplomatically accredited to the host country, to be sure, but still there as observers and reporters on matters of military intelligence interest."[15]

National Security Agency

President Truman authorized creation of the National Security Agency (NSA) in 1952. Although it is a Department of Defense (DoD) agency, NSA collects, processes, and disseminates signals intelligence data "for national intelligence purposes in accordance with guidance from the Director of Central Intelligence."[16] This includes economic-related information.

Signals intelligence (SIGINT) incorporates two sub-sets of intelligence known as electronic intelligence (ELINT) and communications intelligence (COMINT). This thesis is concerned with COMINT: "technical and intelligence information derived from foreign communications by other than the intended recipient."[17] "Foreign" means non-U.S. in origin and includes individuals, companies, and governments. "Communications" includes telephone, Morse code, telegraph, facsimile, wire and optic cable, computers, radio, television, etc. The phrase, "by other than the intended recipient," means that one (in this case NSA) intercepts the communications surreptitiously, i.e., without the knowledge and consent of the communicating parties.

In short, NSA listens to the world's communications to extract information of intelligence value for the USG's policy makers: the President and the National Security Council. NSA provides extracted information to the other intelligence agencies for their analysts to evaluate and incorporate into finished intelligence reports. It employs approximately 30,000 people; its budget is estimated at $13 billion annually.[18]

Providing insight into the agency's capabilities, in 1990, then Director Vice Admiral Studeman discussed NSA's possible role in economic intelligence as eavesdropping on foreign companies to learn about product

lines, sealed bids, new technologies, and on foreign countries' for national economic policy information.[19] Chapter 5 contains a case where such information was used in support of national policy.

Department of State

The Department of State's intelligence ability is located in the Bureau of Intelligence and Research (INR). INR's abilities are limited; none of its approximate 330 personnel are stationed overseas, they work in Washington, D.C. "The Bureau does not collect intelligence beyond reporting through normal diplomatic channels and open source collection."[20] With this basic capability,

> The Office of Economic Analysis produces reports for policymakers on current and longer range issues involving international economic policies, business cycles, trade, financial affairs, food, population and energy, and economic relations....[21]

Department of State analysts review CIA draft reports on political and economic matters for accuracy based on information INR may have that CIA analysts do not. Agency cross reviews are part of the competitive analysis process described earlier.

Department of Treasury

"The Department of Treasury overtly collects and produces intelligence related to U.S. foreign economic policy...."[22] Its analysis focuses on economic trends, financial policies, and the status of foreign economies. Treasury's Office of Intelligence Support publishes figures on foreign Gross National Products, deficits, trade gains or losses, and major industries.

Other Agencies with Economic Reporting Responsibilities

Department of Commerce

The Department of Commerce is not a member of the Intelligence Community. Commerce assesses the foreign availability of high technology products to the former Soviet Union and China, and embargoed countries such as Iran and Cuba.

The Department's capabilities include knowing which countries and companies manufacture or sell high-technology goods, their level of production technology, and foreign export laws. Commerce also analyzes foreign trade data and establishes patterns and profiles of illegal diversions and acquisitions of high-technology goods. The data on goods, technologies, and foreign transactions comes from the "[the U.S.] national labs, government scientists and engineers, foreign commercial groups and data bases, and the U.S. Intelligence Community."[23]

Commerce has access to commercial U.S. information on foreign companies not available to the IC. The Foreign Direct Investment and International Financial Improvement Act of 1990 allows Commerce's Bureau of Economic Affairs (BEA) to obtain census data on individual companies. For example, the BEA can get and analyze data on how many cars and trucks were purchased each year in a given state and which foreign company manufactured the vehicles. "More specifically, the legislation requires a comparison of foreign- and domestic-owned business with regard to 'employment, market share, value-added productivity, research and development, and investment services and services provided.' "[24]

Deputy Under Secretary of Defense for Acquisition

The Department of Defense maintains information on the technological level of nations involved in high-technology fields. The Export Administration Act of 1979 directs the Deputy Under Secretary of Defense for Acquisition (International Programs) to assess the status of foreign technologies designated militarily critical (defined in Appendix A). These assessments include the level of research and development and manufacturing capabilities of other nations and compares their status to that of the United States.

The program receives input from the military services, the Intelligence Community, the National and Service Laboratories, the Department of Commerce, and the Department of State. Table 3 depicts the assigned analytical and reporting responsibilities. The Institute for Defense Analyses, a federally-funded research center, coordinates compilation of the material and publishes the final studies. Most of the reports are available from the Department of Defense.

According to the Institute, DoD's rationale for monitoring foreign programs includes security and competitiveness issues: "Better understanding of underlying foreign capabilities--and what can be done with them--improves our ability to analyze and predict the potential long-term economic impact of technology security and export control policies."[25]

To ensure these studies are thoroughly coordinated and accurate, DoD involves 350 industry representatives and 550 government personnel.[26] Participation is based on specific technology expertise; not all 900 personnel work on each report.

TABLE 3

TECHNOLOGY TRANSFER RESPONSIBILITIES [1990]

ORGANIZATION	RESPONSIBILITY
Deputy Under Secretary of Defense (International Policy)/DUSD(IP)	Technical Framework & Foreign Technology Assessment
Under Secretary of Defense for Policy/USD(P)	Policy Overlay
Joint Chiefs	Strategic Rationale
Intelligence Community	Assessment of Capabilities of Nations
Military Services	Expert Inputs from [National] Labs/[Military] Commands
Institute for Defense Analyses	Federally-Funded Research & Development Center Providing USDA with Technical Support & Analyses

Source: U.S. Department of Defense, Deputy Under Secretary for Defense of Defense for Acquisition (International Policy), Technology Identification and Analyses Center FY 1991 and FY 1992 Report (Alexandria: Institute for Defense Analyses, January 1993), III-1.

The foreign assessments do not list the capabilities of individual companies within countries. The 15 technology categories that DoD assesses and two assessment charts are depicted in Appendix B.

Summary

The DCI heads the U.S. Intelligence Community, a group of government agencies with specific assigned responsibilities, under centralized control. The basic IC elements with economic-related collection and reporting responsibilities are: the Central Intelligence Agency, the Defense Intelligence Agency, the National Security Agency, the Department of State's Bureau of Intelligence and Research, and the Department of

Treasury. Two other non-IC elements, the Department of Commerce and the Under Secretary of Defense for Acquisition, have legal responsibilities concerning economic intelligence. Some of these intelligence entities have more involvement in economic intelligence than others. The cumulative capabilities of these agencies allow for a wide range of economic reporting to support national policy makers.

CHAPTER 5

ANALYSIS OF THE U.S. GOVERNMENT'S CAPABILITIES

Overview

To evaluate the U.S. Government's intelligence activities, first, the strengths and weaknesses of the primary intelligence collection methods will be analyzed. The qualities possessed by the collection methods impact on the quality of the resulting intelligence. Second, the ability of the USG to collect and analyze economic-related intelligence (as described in Chapter 4) will be evaluated against the following criteria: accessibility, accuracy, cost, releasability, and timeliness. These criteria were selected due to their potential value to business with respect to information.

Collection Methods

The various "INTs" merit more attention than the descriptions given in Chapter 4. Each collection method has advantages and disadvantages associated with it. These qualities and limitations exist regardless of whether the employer of the discipline is private industry or government. In turn, each method's inherent qualities and limitations impact on the accuracy, accessibility, cost, releasability, and timeliness of government intelligence.

Human Intelligence

This collection method is available to most organizations. It relies on nothing more sophisticated than having an individual or individuals placed or recruited within the "target" business.

HUMINT comes with inherent disadvantages. Agents can fabricate information or repackage and embellish publicly available information to make it appear that it came from high-placed sources in order to sell it.[1] Another possibility is that the agent is a double--secretly working for the designated target company or foreign government and providing deceitful information back to the parent company or government.

An advantage of HUMINT is target accessibility. While it may be difficult to recruit a well-placed agent within a corporation, once done, the informed agent might have access to R&D, marketing, contract, or company policy information.

Communications Intelligence

The National Security Agency conducts the bulk of communications intelligence for the IC. CIA also intercepts communications, though this activity is not its primary collection business. America's COMINT abilities are familiar to other countries. Alexandre de Marenches complimented the U.S. on its technical (non-human) collection means. "In that area--the spy [imagery] satellites and electronic monitoring through the National Security Agency--the Americans have always had an unparalleled capability."[2]

NSA receives COMINT through several means. Satellites, electronics-equipped aircraft, and ground based intercept sites provide access to microwave, computer, telephone, radio, etc. communications. Specific

examples of NSA intercepts will be described later. CIA locates its COMINT activities in U.S. embassies and consulates. The listening post in the U.S. Embassy, Moscow intercepted a conversation, in the early 1970s, between General Secretary Brezhnev and Field Marshall Grechko. Grechko told Brezhnev that heavy Soviet SS-19 missiles would fit inside launch tubes of lighter SS-11 missiles, making them permissible under the SALT I treaty.[3]

COMINT has some drawbacks. First, it is a passive collection method. Whereas in HUMINT and OSINT, individuals actively seek information, with COMINT, if the collection target does not use his communications, no collection is possible. Second, if the target becomes aware that his communications are being monitored, he may interject false information to deceive the interceptor.[4]

A final consideration with COMINT is the volume of material intercepted. Running continuous world-wide operations, the COMINT collection agencies gain, "unbelievable box-car loads of tapes...."[5] At present, computers automatically screen intercepts for key words. Selection of transmissions through key words, for example "contract," "bid," "computers," or "aerospace," might still yield hundreds of conversations daily. Transcribed conversations require an analyst read them to determine content value. If a transcription is considered worthwhile, the analyst will attempt to cross-check its contents with other related and on-hand information. This can entail telephone calls or visits to other analysts and agencies, computer data-base checks, and library searches. Having done this, I can attest that the process is incredibly time-consuming.

Imagery Intelligence

Imagery intelligence (IMINT) entails producing an image, whether a standard black and white photograph, radar or infrared picture, or display on a computer screen. The image depicts something on the face of the Earth, vehicles, ships, or buildings, and is photographed from a platform located in either the atmosphere or space. The formal definition is located in Appendix A.

The U.S. Intelligence Community obtains imagery from space-based satellites and specially-equipped aircraft. America first acknowledged an imagery capability in 1960, after the Soviet Union shot-down pilot Gary Powers in a U-2 aircraft during a reconnaissance flight over that country. In 1978, President Carter confirmed the existence of U.S. imagery satellites when he showed pictures of Soviet ICBM missile sites on national television.[6]

Past imagery reconnaissance missions in support of U.S. security interests include: monitoring the 1986 Chernobyl nuclear power plant accident in the Soviet Union; observing the development of a new long-range Soviet bomber at Ramenskoye airfield in 1981; and observing batteries of SA-2 and SA-3 surface-to-air missiles being unloaded from ships at the Cuban port of Mariel in 1985.[7]

U.S. imagery assets have long monitored the defense industrial base of selected nations. Imagery systems watched defense factories in the Soviet Union: the Kharkov tank factory; the Ramenskoye Airfield test center; the Nikolayev ship-building yards; and the R&D missile facilities at Sary Shagan.[8]

To support economic intelligence, imagery collection has the potential to watch civilian factories in the same manner. IMINT can show

the external lay-out of a factory or plant complex, the level of factory activity, deliveries of materials or components, and finished products of the plant stacked or parked outside.

But IMINT has limitations. Assets cannot remain over the target indefinitely nor can they look through cloud cover.[9] Time-dependent activities, the delivery of raw-materials, activity levels, and finished goods movements, can be observed only if the aircraft or satellite flies over the target the same time the activity occurs. Furthermore, satellite paths can be calculated and times-over-the-target predicted. The target can either cover outside activities or materials or schedule his activities to avoid overflight.[10]

The manufacture and deployment of satellites, imagery and communications intercept, is expensive. The National Reconnaissance Office (NRO) manages the building and fielding of intelligence satellites.[11] In 1992, the estimated budget of the NRO was $6.2 billion dollars, the single largest slice of the U.S. intelligence budget (see Table 4).

Imagery also cannot reveal a company's policy plans or intentions, contract or marketing details, and research and development plans or programs under development. Human intelligence, communications intelligence, and open source intelligence are more likely to provide this information.

Open Source Intelligence

Open source intelligence (OSINT) comes from publicly available material: newspapers, books, magazines, radio and television broadcasts, information services, and so on. The more open the society, such as the United States, the more information is available. In the United States many

business documents, statements of ownership, profit and loss statements, and year-end summary reports, are available to the person who knows where to find them. The following two cases illustrate the ease of an open source business search in the United States.

Throughout the 1980s, Japan has gathered information on the aerospace field, specifically, satellite and rocket production. The U.S. National Aeronautics and Space Administration (NASA) has fielded over 1500 Freedom of Information Act (FOIA) requests from Japanese sources. These sources include Mitsubishi employees, and Mitsubishi's American consultants and legal firms. "Information obtained through the FOIA is believed to have helped Mitsubishi Electric Company substantially in its development of its H-2 booster rocket and its earth resources satellite, ERS-1."[12]

In the second case, one private researcher examined a foreign automobile manufacturer entering the U.S truck market. Her goal was to get information on the company's truck and its marketing plans. She discovered the truck's design, its sell price, its approximate production costs, the manufacturer's production goals, the type of manufacturing equipment to be used, manufacturing plant specifics (to include blueprints from a local government agency), and how much money in tax incentives and public monies for support facilities would be available to the manufacturer. The researcher also made a directory of the manufacturer's top executives, with a listing of their strengths and weaknesses.

To get the information, the individual "...consulted 14 published sources (ranging from local newspapers to the International Directory of Corporate Affiliations), six Federal regulatory agencies, six state agencies,

one local agency, and seven company watchers (among them local Chamber of Commerce officials and trade-magazine reporters)."[13] That the researcher conducted this search entirely in the United States is important. It is more difficult to get information such as this from inside a closed society, but information can still be obtained through foreign libraries, government offices, and on-line business and technical information services such as Dialog and Internet.

The massive amount of information available through open sources is both an advantage and disadvantage. Although some key corporate information is available through persistent hard-work, it can be time-consuming and expensive. The search described above took 80 hours and cost $1500 dollars. This particular cost is relatively inexpensive, but consider that it was done in the United States and most information was gained for the price of several telephone calls.[14]

To conduct this search in a foreign country, would cost considerably more. A company must hire an individual familiar with local and government laws and proficient in the country's language. A researcher would also not likely elicit free information either but would be expected to pay for it. Then there are associated costs for working space, computers, telephones, and subscriptions to data-bases. For an entity such as the USG to search for, translate, and scan open source material from around the world and in a variety of industries, then double-check its accuracy against classified information, would probably require hundreds of employees with computers. Such an effort would not be inexpensive or quick. In 1990, there were 4465 commercially-available data-bases world-wide.[15]

Fusion

Each intelligence collection method has strengths and weaknesses associated with it. HUMINT, COMINT, IMINT, and OSINT do not support analysts or decision-makers, national or corporate, in isolation. Information sourced from these "INTs" is pieced together to form as complete a picture as possible of the target.

The collection methods can complement each other; in this way limitations can be minimized and strengths capitalized on. For example, an agent placed within a corporation may provide information on plans to build a nuclear power plant in another country (HUMINT). The intercept of telephone conversations and facsimile transmissions may provide details on contract negotiations, sub-contractors involved, bids proposed, and contracts won (COMINT). One may find proposed plans and blueprints at a local government office that requires the filing of plans before building permits are issued (OSINT). Finally, photos may confirm construction start-up at the plant site (IMINT). No one or two collection methods could provide all this information, but the fusion of several methods can.

Accuracy

It is difficult to assess the accuracy of the Intelligence Community's economic-related studies. Most of its products are classified and, therefore, are not available for analysis. Publicly available CIA products concentrate on strategic level economic trends and statistics of select nations and geographical regions. These support policy-makers with broad foreign economic information. "The questions considered by government intelligence

analysts are largely not about [specific] products and markets which are usually of greatest interest to businessmen."[16]

Appendix C, Government Documents Available, lists a sample of CIA documents that can be purchased; this list shows the national-level focus of the agency's collection and analytical efforts.

Discussion: Criticism

Of the CIA's assessments that can be critiqued, the results are mixed. The IC has sustained some public and notable failures. A passage from National Security Strategy summarizes some major past inaccuracies:

> In the late 1980s and early 1990s, the record of the intelligence community seemed particularly poor. It predicted that the Soviet-backed regime in Afghanistan would fail within weeks of the Soviet withdrawal (it lasted five years); it failed to predict the speed of the collapse of the Soviet Union and the Soviet empire; and it failed to give adequate warning to the Bush administration in 1990 of Iraq's aggressive intentions and clear preparations for the invasion of Kuwait.[17]

In addition to these instances, CIA's analyses of the 1970's and 1980's of the Soviet Union and Soviet-bloc economies have come under strong criticism for their inaccuracies. In one example, "Senator Moynihan...tells the story about CIA [analysts] coming into the Senate Intelligence Committee just two years before the fall of the Berlin Wall and telling the...Committee that the East German per-capita income was greater than the West German per-capita income."[18] One former CIA officer said, "I don't remember an oil [production] estimate we ever got right."[19]

Discussion: Praise

Conversely, the CIA has received high praise in some quarters for its analysis of Japanese trade negotiations and predictions of Japan's international gains. According to a former Department of Commerce trade negotiator,

> Of all the agencies in Washington, the Central Intelligence Agency had perhaps the clearest, most comprehensive view of Japan. Its analyses and forecasts were usually borne out by events. It did not believe that Japan shared U.S. economic views, and foresaw that neither devaluation of the dollar nor stimulation of Japan's economy would resolve U.S.-Japan trade problems. It particularly feared growing U.S. technological dependence and urged vigorous support of U.S. industry. Its reports were largely ignored.[20]

Former DCI Stansfield Turner feels that the CIA has a record "...of very, very good performance in the economic area."[21] In a counterpoint to Senator Moynihan, Admiral Turner commented, during a television interview, that CIA analysts accurately predicted the decline of the Soviet economy but senior political analysts, himself included, failed to interpret the information properly. Personal biases on the topic led him to reach a different conclusion than the analysts.

A former NSC staffer recounts when the CIA economists made an accurate assessment.

> A decade ago, top NSC officials, unnerved by the Treasury Department's complacency about the Third World debt buildup, asked the CIA to assess the problem. In a report to then-President Reagan, the agency described the debt overhang as bigger and more destabilizing than the Treasury was acknowledging. 'The CIA was right, but nothing ever happened,' recalls former NSC staffer Gregory Treverton,...'Treasury policy prevailed.'[22]

Accessibility

One consideration in the ability of any agency or company to obtain information is its accessibility to the desired information. With the extensive collection and analytical systems and staffs, the Central Intelligence Agency and the National Security Agency have unique access to sources not readily or legally available to companies or businessmen.

Some USG personnel admit this. A deputy director of the White House Office of Science and Technology Policy [during the Bush administration], Michelle Van Cleave, has said, "...the Intelligence Community has the ability to provide commercially useful information such as details about competitor firms, advanced plans for major foreign projects, financing arrangements and government and industry research projects."[23]

Remarks made by DCI Woolsey, in a 1993 interview, indicate that today the CIA can and does collect information on who in a foreign country is bribing someone else in order to get contracts and cut out U.S. competition.[24] Sometimes this information is passed to the State or Commerce Departments which in turn can intercede with warnings to a foreign government to ensure equitable access to contracts by all bidders.

Former DCI Stansfield Turner, in an August 1992 television interview, related that a CIA Chief of Station told him about two foreign companies bidding against an American company on a major contract in an unnamed country.[25] These comments from former and current government officials reveal that the Intelligence Community has access to contract and financial information within foreign companies.

Cost

Determining the cost to collect and analyze any category of intelligence cannot be done accurately. The U.S. Intelligence Community budget remains classified. The Congressional appropriations committees that approve the funding for U.S. intelligence activities conduct their budget hearings in secret. Estimates of the U.S. intelligence budget have been made by individuals who have collated comments from knowledgeable Congressman and other government and Department of Defense officials. Portions of one such estimate are depicted in Table 4.

TABLE 4

U.S. INTELLIGENCE COMMUNITY BUDGET
(Estimates, in millions of dollars, for 1992)

National Reconnaissance Office	6,200
National Security Agency	3,900
Central Intelligence Agency	3,200
Defense Intelligence Agency	582
Intelligence Community Staff	100
State Department (INR)	50
Total	14,032

Source: Adapted from Larry Grossman, "Intelligence in a World of Change," Government Executive, March 1992, 12.

Note: The National Reconnaissance Office builds and manages the satellites that collect communications signals and imagery. This table does not reflect the total USG intelligence budget. The Intelligence Community Staff is made up of senior officials, some of them Presidential appointees, who provide policy guidance to the IC.

As noted previously, former DCI Gates indicated that approximately 40 percent of the information collected by the Intelligence Community relates to economic matters. Given the $14 billion dollar budget above, this equates

to approximately $5.6 billion dollars expended toward the collection and analysis of economic information.

Current and future cost issues relate to the size reduction of the United States Government initiated during the Bush administration. In a 1991 speech given while he was DCI, Robert Gates said that, "The CIA has already begun a 15 percent personnel cut through attrition over the next several years, and projected budgets have been slashed by billions of dollars...."[26] Personnel and budget cuts have also been implemented at the National Security Agency and the Defense Intelligence Agency.

Government intelligence organizations already have operationa collection assets and thousands of analysts. If economic intelligence analysis received increased attention, internal assets would require redirection to expand analysis and reporting functions. Private corporations either hire consulting firms or hire and train their own staffs to conduct intelligence work.

Profits gained from economic intelligence also cannot be calculated. To judge from comments made by the French former intelligence official, Alexandre de Marenches, the gains to a country can be figured in the millions of dollars (Chapter 3). A U.S. case of economic intelligence discussed at the end of this chapter concerns the awarding of a contract worth $50 million dollars to a U.S. subsidiary company.

DCI James Woolsey indicated in a 1993 interview that the U.S. intelligence agencies are assisting the profit gains and competitiveness of U.S. companies, if indirectly:

> I would say today [30 November 1993] billions of dollars a year are saved in contracts for American companies by the State Department or the Commerce Department being able to go to a foreign government and

saying "You'd better be careful. On this contract we understand 'X' country or 'X' company is trying to bribe its way into getting that contract. You'd better play straight." That happens quite a bit now, and it's something we have a major hand in.[27]

This policy is known as "leveling the playing field." It is intended to allow honest and open competition in foreign markets. It does not mean the U.S. company gets the contract, only that it gets a fair chance at it. Benefits to U.S. industry cannot be determined from this shadow assistance. A company would never know the USG interceded with a foreign government on its behalf unless government officials admitted to it.

Congressman Craig James displayed concern about different cost factors in a 1992 Congressional hearing on foreign economic espionage:

> This [U.S. economic espionage] would be a very direct but hidden cost to business, to the taxpayer, under the guise of economic espionage or protecting business interests when we consider the international aspect of business and foreign ownership of stock, foreign control and sometimes you can't even determine either of those. Just look at the components of a car, and you will see already how involved internationally many products are.[28]

It is difficult to define what makes a company U.S. or foreign. But international economic espionage has been conducted for decades; foreign countries and companies seemingly do not constrain their activities based on stock ownership or foreign control. From the discussion of foreign economic espionage in Chapter 3 with de Marenches' comments about profits gained and DCI Woolsey's comments concerning billions of dollars in contracts garnered for U.S. industry, the price of conducting economic intelligence more than appears to pay for itself and outweigh any business or disclosure risks.

Releasability

Intelligence Community analysts routinely concern themselves with the appropriate classification of information. After information is classified (based on guidelines that deal with the way in which it was collected and the damage its release may cause to national security), collated, analyzed, and distributed as intelligence, the mention of releasability can cause consternation. Members of the Intelligence Community are concerned that to release intelligence to an individual or agency at a lower classification level or in an unclassified form will compromise the source or sources of the information.

Distrust can arise from perceived over-classification of reports and the resultant diffuseness of intelligence when it is released at lower levels. Once all indications of the intelligence source have been deleted, the resulting reports can be too vague to be useful. "Persian Gulf Commander General Schwarzkopf noted in his report to Congress that the analyses from [U.S.] intelligence agencies were so 'caveated, footnoted, and watered down that we [the forces] would still be sitting over there if we were dependent on that analysis.' "[29]

Information can be released with deletion of the source or collection means. There might be instances where information is so specific it could only come from one source, an in-person conversation, telephone call, or written report, and it cannot be attributed plausibly to another source. In this case, the agency would decide not to release the information to protect the source for continued access. If the information could come from a combination of sources, trade journals, a computer information net, telephone

conversations, and several knowledgeable individuals, the IC is more likely to authorize release, even to the public, i.e., non-government individuals.

Timeliness

A case from the early 1980s demonstrates timeliness and accessibility of the U.S. Intelligence Community to get information that a private business or researcher could not. Although this incident does not involve economic intelligence, it reveals how foreign companies and their governments cooperate in espionage activities. If the USG and private industry ever shared information, this could be one way. Finally, it shows the cooperation and information sharing between U.S. Government agencies.

Sources at the National Security Agency revealed that on 13 July 1982, NSA intercepted communications transmitted from Mitsubishi's Washington, D.C. office to the Japanese Foreign Ministry in Tokyo. The intercepted communications contained classified information from CIA authored reports written for the president and national U.S. policy-makers. NSA intercepted additional communications between Mitsubishi and the Foreign Ministry on 29 July and 4 August. Information contained in the reports included military and political analyses of the on-going Iran-Iraq War and political developments in the Soviet Union.

NSA alerted the FBI to the security breach; the information could only have come originally from a USG source. In the communiqués, Mitsubishi had said that it got the reports from a Washington, D.C. consulting firm that in turn got them from a senior U.S. intelligence official. Suspicions centered on one individual who eventually resigned his position at the CIA. The FBI could not prove conclusively who leaked the information,

but after the CIA employee resigned, Mitsubishi's reports to Tokyo no longer contained classified information.[30]

This case highlights access by the Intelligence Community: NSA's ability to eavesdrop on ostensibly private communications. It also demonstrates timeliness. NSA analyst's read the information on the same day it was intercepted. Officials at NSA alerted the FBI to the security problem shortly thereafter. If in fact the one CIA official leaked the information, the FBI investigation against him prompted his resignation; the security problem disappeared rapidly.

Analytical Elements

The Intelligence Community has large staffs of analysts. Most of them work at the big three: the Central Intelligence Agency, the National Security Agency, and the Defense Intelligence Agency. If Jeffrey Richelson's estimates in The U.S. Intelligence Community are correct, the three agencies have approximately 55,000 employees total. The agencies do not publish the size of their agencies or a break down of staff numbers. But if one figures that up to 50 percent of the personnel work in collection-related activities and support functions (personnel, training, computer support, classification guidance, liaison with outside agencies, etc.), then there may be as many as 27,000 plus individuals engaged in intelligence analysis.

A congressional directed study considered that an important capability of intelligence agencies rests within "...established analytical staffs with collective memories on economic and scientific and technical matters that have been built up over a significant period."[31] As described in Chapter 4, DIA hires engineers and technically-trained specialists to conduct S&TI

analysis. The CIA has economic specialists on its analytical staff. In 1991, a CIA spokesman admitted that the agency was hiring more economists. He said that CIA's future focus [with additional analysts] would be: [international] economic capabilities and constraints, trade and financial strategies, and technology.[32]

Business likely has a difficult time building this collective expertise. Plus, no one company or group of companies could afford an analytical staff of such a size. Government employees often like the stability of working for one employer and accruing seniority and experience. Private industry maintains a higher turnover of personnel through mergers, down-sizing, and individual career desires to seek employment elsewhere.

A Summary Case

In 1990, senior U.S. Government policy-makers, including President Bush, made an apparently rare decision to use USG economic intelligence to help a private business. The CIA Chief of Station (senior CIA official in country) in Jakarta, Indonesia received information from a source in the Indonesian government that a contract for $100 million dollars would be awarded to the Japanese electronics firm, NEC. The contract was to modernize Indonesia's national telephone system; the contract had been open for bids around the world.[33]

Central to the issue, the Indonesian source reported that American Telephone and Telegraph's (AT&T) European subsidiary had submitted a more attractive bid: better improvement specifications for a lower cost than NEC. Under "normal" circumstances, Indonesia would have awarded the contract to AT&T. Reportedly, Japan threatened to reduce its foreign aid to

Indonesia, valued at $2.1 billion dollars, if a company other than NEC received the contract.[34]

The CIA Station Chief forwarded the information to Washington, D.C., and CIA senior officials presented it to President Bush. The President wrote a letter to President Sukarto of Indonesia concerning the matter. He reminded President Sukarto of America's commitment to and long-standing commercial ties with Indonesia. Two weeks later, Indonesia split the contract in half between NEC and AT&T.[35] In this publicized incident, the elements of accessibility, accuracy, and timeliness were present and benefited the United States and AT&T.

The cost to the USG of this operation cannot be calculated; the CIA does not disclose the price to obtain information from foreign government officials. Profits, however, can be figured at $50 million dollars for AT&T. Although the European subsidiary obtained the contract, some profits are probably involved for the parent U.S. corporation. President Bush would not likely have become actively involved otherwise.

On 29 April 1994, DCI James Woolsey acknowledged the CIA continues to collect and provide this type intelligence to government leaders on behalf of U.S. economic interests. He stated that whenever the agency obtained information on international business improprieties, the USG would "level-playing field." As in the above case, this means the USG will tell the involved foreign government to ensure business is conducted fairly and allow U.S. companies an equal chance to compete for contracts. [36]

Conclusion

The Central Intelligence Agency and the National Security Agency conduct the majority of economic-related intelligence collection and analysis within the United States Government. These large agencies possess collection assets giving them access to detailed economic information from foreign companies and governments. From the above examples, the USG demonstrated the ability to collect and analyze economic information quickly and give it to senior government officials for action.

Although the Intelligence Community has received criticism for inaccurate analyses, some open source examples demonstrate success. Some of the positive incidents described here have been publicized by individuals who had little to gain from supporting the Intelligence Community. Clyde Prestowitz, the Counselor for Japan Affairs (Department of Commerce, 1983-1986) gave the CIA uncharacteristic praise for its analysis of Japan's financial strategies. Former DCI, Stansfield Turner criticizes himself and other senior government policy officials for ignoring CIA's assessments. Finally, the head of a foreign intelligence service praised NSA's capabilities as "unparalleled" in the world.

Treasury, Commerce, and State can provide information on foreign financial policy, foreign and U.S. export laws, and long-range international monetary trends. They do not currently have the staff size or unrestricted access into the main intelligence players to provide intelligence to business on their own. Directions to these two departments to conduct economic intelligence would require a mission restructuring and staff expansion. At best, the Intelligence Community could funnel economic intelligence through the Departments of Treasury or Commerce to private industry.

A former CIA analyst provided the most succinct comments about the Intelligence Community's potential to support business with economic intelligence:

> Were the CIA assigned the task of filching economic secrets overseas...its operatives could easily help push a Japanese computer company or a European aircraft manufacturer out of international competition. We'd be so good at it...it would be frightening. [37]

Summary

The U.S. Intelligence Community has the collection and analytical capabilities to provide economic intelligence to national policymakers and, if directed to do so, to U.S. corporations. Research for this thesis discovered that the Intelligence Community, in fact, already conducts extensive economic intelligence activities to support national security concerns. The Central Intelligence Agency and the National Security Agency provide the majority of the collection and analytical effort to economic intelligence. They have access to collection opportunities and can provide accurate and timely intelligence analyses to government officials. President Bush, on one acknowledged occasion, used economic intelligence to benefit U.S. industry.

CHAPTER 6

CONCLUSION

Final Analysis

The United States Government (USG) already collects and uses economic intelligence. The Intelligence Community focuses on "providing American policymakers information on what other governments are doing that effect U.S. economic interests."[1] U.S. policymakers have, at times, used this intelligence to benefit the U.S. economy and individual companies.

The two largest U.S. intelligence agencies, the Central Intelligence Agency and the National Security Agency, collect, and analyze most of the economic intelligence conducted by the USG. The Defense Intelligence Agency analyzes and publishes Scientific and Technical Intelligence (S&TI). The Departments of State, Treasury, and Commerce perform a limited analytical role in economic intelligence. They do not have true collection capabilities, such as the CIA and NSA, nor sufficiently-sized staffs to conduct in-depth analysis.

The primary Intelligence Community reporters of economic intelligence, the CIA and NSA, can provide accurate and timely analyses to government policy-makers. If directed to do so, these agencies could release intelligence to corporations fast enough for the companies to use it to their competitive advantage.

Relationship to Previous Studies

Previous studies related to USG involvement in economic intelligence center on one of the following issues:

1. The economic espionage activities of allied nations.

2. The erosion of American preeminence in select high-technology fields.

3. The relationship between the health of industry and the economy to national security.

4. The legal and policy issues concerning the provision of USG generated intelligence to private business.

Books and reports that discuss these issues are: Friendly Spies, The Threat of Foreign Economic Espionage to U.S. Corporations, The Fourth World War, and Dans le Secrets des Princes (allied economic espionage); Selling Our Security, Powershift, American National Security, and "Technology and Competitiveness: The New Policy Frontier" (America's competitiveness decline and its relation to national security); National Security Strategy and Technology Proliferation and U.S. Technological Superiority (industry and national security); and The Threat of Foreign Economic Espionage to U.S. Corporations and The U.S. Intelligence Community: A Role in Supporting Economic Competitiveness (policy discussions).

Other authors describe the basic capabilities and functions of the Intelligence Community but provide no details on its ability to conduct economic intelligence. Basic references include: The U.S. Intelligence Community, Silent Warfare, Deep Black, and American National Security.

This thesis fills an information gap left by current studies and books. A link is made between the importance of economic competitiveness to national security and the damage done to U.S. industry and national security by foreign economic espionage activities. Collection and analytical capabilities of the Intelligence Community are described with a view toward their ability to provide detailed and effective economic intelligence to industry. Examples of acquired economic intelligence highlighted capabilities of the U.S. Intelligence Community.

Previous studies did not make linkages between the IC's capabilities and its ability to conduct economic intelligence. This thesis incorporated information from the sources listed above and from sources not available until recently. Past DCIs, the senior intelligence official in the United States, and the current DCI have appeared on television interviews and discussed economic intelligence and national policy concerns. The Defense Intelligence Agency presented an unclassified paper to the Joint Chiefs of Staff about intelligence and technology concerns.

Suggestions for Further Research

Other related issues were discussed in detail here. Issues that would benefit from further study are:

1. Would the provision of USG intelligence to private industry require changes in federal (intelligence or business) laws and executive orders? Some officials, such as Senator Moynihan and former DCI Robert Gates, suggest it is illegal for the USG to provide intelligence to private industry. Their comments did not clarify what particular legal problem exists. Author Peter Schweizer (Friendly Spies) may have identified the

problem: "This country has on its books antitrust laws that prohibit the government from favoring or aiding particular companies and industries." [2]

Having no legal background, I cannot address the accuracy of his statement; however, in view of past government support to certain industries, Schweizer's comment seems questionable. The USG provides subsidies to some farmers, grants tax incentives to businesses, and loaned money to Chrysler Corporation to keep it from bankruptcy. This legal issue deserves in-depth research.

2. If the USG provided economic intelligence to companies, through what mechanisms would it be disseminated? Would the Central Intelligence Agency or National Security Agency would provide select intelligence directly to business? This is not likely to occur. Another idea might be for the agencies to pass intelligence through the Department of Commerce. Perhaps a national standing review committee could be established to evaluate the intelligence provided by CIA, NSA, and DIA; the committee might decide whether the information should be given to industry, and if so, to which companies.

As a sub-issue, would individual companies submit requests for information to initiate collection or analysis? Or would companies rely solely on the intelligence agencies to determine what to collect? What are the implications for a General Motors to ask for specific research, marketing, and contract data on Mitsubishi's plans to compete against General Motors in Argentina.

3. Which U.S. companies would receive economic intelligence? Potentially, the IC would be overwhelmed trying to provide intelligence to all industries or requesting companies. Limits would need to be imposed on who

gets access to foreign competitor information. It might require a presidential commission made up of business, government, and intelligence officials, to study the problem and recommend parameters. One limitation might be that only those companies which research, develop, and manufacture in high-technology industries receive government support. Technologies designated important to national security, such as those listed in the Militarily Critical Technologies List, would be the prime candidates to benefit from government assistance.

4. What defines a U.S. corporation? Is it a company whose stock is held solely by Americans? What if 10 or 20 percent of the stock is held by foreigners? What about companies owned by foreigners that are based in the United States and managed by U.S. citizens? What about providing intelligence to the foreign subsidiaries of U.S. companies? What about U.S. companies conducting joint ventures with foreign companies (such as the FSX fighter)?

Former DCI Robert Gates summarizes the problem,

> It's a terrible practical problem. Which companies are we going to help? Which industries are we going to help? How much of our resources should we sink into it? It's a bottomless well. I think it's an illegal morass.[3]

Rather than saying, however, that all the described problems are too hard to cope with, they could be analyzed separately with a view toward how they impact on the issue.

Finally, little information is publicly available on past instances where the USG has used intelligence to assist U.S. corporations. Cases such as the one in Chapter 5, when President Bush contacted Indonesia to ensure equal contract consideration for a U.S. company, do not come to light unless the USG releases previously classified information. This case was the only

one found during thesis research. Consulted databases included: LEXIS (newspaper articles), DIALOG (business information), and ABI/INFORM (periodicals). Information searches covered from January 1986 to April 1994. CIA and DIA were also contacted. The CIA was not able to provide information for this thesis. DIA provided limited assistance. The disclosure of additional cases could provide future researchers with important information for analysis.

Summary

The United States Government, through the U.S. Intelligence Community, can collect and analyze economic intelligence suitable for use by private industry. Through past actions, the U.S. Intelligence Community has proven it can get access to information to provide accurate and timely intelligence to those who need it to. The cost of maintaining a large government intelligence community runs into the billions of dollars yearly; however, economic and national security gains would probably offset the expenditures.

This thesis fills an information gap between other studies dealing with related aspects of the economic intelligence issue: U.S. competitiveness, foreign economic espionage, descriptions of the U.S. Intelligence Community, and the link between national security and the national economy. It addresses the actual capabilities of the U.S. Government to conduct economic intelligence. Legal, definition, and dissemination problems need to be resolved before U.S. Government intelligence could be released to private industry. Other studies remain to be done to address those issues and provide possible solutions.

APPENDIX A

DEFINITIONS

The terms for competitive intelligence and economic espionage were compiled from several sources. Like the term economic intelligence, no authoritative definitions have been published. These composite definitions are in keeping with generally accepted meanings of the terms.

1. Communications intelligence (COMINT). "Technical and intelligence information derived from foreign communications by other than the intended recipient."[1]

2. Competitive intelligence (CI). Competitive intelligence is information collected and analyzed on businesses and business markets and meant to give the information holder an advantage over competitors. It includes the information listed below in economic espionage. Competitive intelligence is often collected from open-source data-bases but can include proprietary information. Open sources can include public tax returns, public financial reports, business periodicals, stock market listings, and on-line computer information services such as Dialog. Some business individuals refer to competitive intelligence as business intelligence (BI).

3. Economic espionage. Economic espionage is the practice of spying on an entity to gain information on its finances, customers, and goods and services. Desired information can include: product or technology research, development, and testing; materials used in and designs of products;

suppliers of materials; buyers or customers; and contract details. Economic spying is done without the consent and, preferably, without the knowledge of the target. Individuals, companies, and national governments engage in economic espionage. Although business personnel often consider economic spying unethical, the activity is not always illegal. Economic espionage was once more commonly known as industrial espionage. Milton Socolar, from the U.S. General Accounting Office, testified before Congress that his definition of economic espionage is the theft of (economic-related) information from U.S. companies by foreign governments.[2]

4. Human intelligence (HUMINT). "A category of intelligence derived from information collected and provided by human sources."[3]

5. Imagery intelligence (IMINT). "Intelligence information derived from the exploitation of collection by visual photography, infrared sensors, lasers, electro-optics and radar sensors such as synthetic aperture radar wherein images of objects are reproduced optically or electronically on film, electronic display devices or other media."[4]

6. Information. Unevaluated material from any source and any medium which may contain intelligence information. The key word in this definition is "unevaluated."

7. Intelligence information. Information with potential intelligence value.

8. Intelligence. The definition of intelligence varies throughout the Intelligence Community based on the focus and customers of each agency. Each definition, however, contains related elements. The DoD definition is: "The product resulting from the collection, evaluation, analysis, integration, and interpretation of all available information which concerns one or more aspects of foreign nations or of areas of operation..."[5]

William R. Corson wrote a useful layman's distinction between the terms intelligence, intelligence information, and information.

> A word of caution about the term "intelligence" is in order. Too often it is used synonymously or interchangeably with "information"....Information until, and unless, it has been analyzed and evaluated remains nothing more than a fact....Intelligence by itself refers to the meaning of, or a conclusion about, persons, events, and circumstances which is derived from analysis and/or logic. Intelligence information consists of facts bearing on a previously identified problem or situation, the significance of which has not been completely established. And information is made of raw facts whose relationship to other phenomena has yet to be considered or established.[6]

9. Militarily critical technologies. These are technologies identified in the Department of Defense (DoD) Militarily Critical Technologies List (MCTL) as being of vital importance to the ability of the United States to maintain military technological superiority. The MCTL lists items as militarily critical "if their acquisition and exploitation by a potential adversary would either: significantly negate or impair a major military capability of the U.S.; or significantly advance a critical military mission area of a potential adversary."[7] These items may be and often are dual-use in nature; that is, they have applications in both military and civilian products or systems. The DoD does not consider an item militarily critical if a potential adversary can manufacture or procure from another country or countries the item in quality comparable to U.S. abilities and in sufficient quantities for its needs.

There are 15 categories of key technologies that include: electronics, telecommunications, industrial production, lasers and optics, propulsion systems, and directed energy systems. The above listed, and nine other categories, are sub-divided into specific critical elements such as related equipment, software, components, and so on.[8] The MCTL key technologies are listed and described in Appendix B. It is important to note that those

technologies that foreign countries and companies target to steal or gain information on are often listed in the MCTL. Because these technologies are considered "high" or sophisticated, are expensive to research, develop, test, evaluate, and produce, and are incorporated into systems that frequently sell for millions of dollars, foreign competitors consider their acquisition of the highest priority. It is no accident, but by a deliberate national plan, that a French intelligence agency targeted U.S. companies to collect information on the production coatings applied to stealth aircraft.[9] Foreign competitors are not interested, for example, in how the Burlington company designs and manufactures towels and socks.

10. Open source information, Open source intelligence (OSINT). "Information of potential intelligence value (i.e., intelligence information) which is available to the general public."[10]

APPENDIX B

MILITARILY CRITICAL TECHNOLOGIES

The Department of Defense has designated 15 categories of technologies as militarily critical. The definition of militarily critical is listed in Appendix A. Briefly a militarily critical technology is one that if acquired and exploited by a potential adversary would negate or impair a major military capability of the U.S. or would significantly advance a critical military capability of a potential adversary. The 15 militarily critical technologies, listed in the Department of Defense Militarily Critical Technologies List (MCTL) are:

1. Materials Technology: This includes metals, alloys, ceramics, composite materials, polymeric materials, electromagnetic radiation absorber materials, magnetic metals, and superconductive conductors.

2. Industrial Production Technology: This includes computer-aided design and computer-aided engineering processes and systems, manufacturing integration, isostatic presses, robots, high-temperature furnaces, and numerically controlled machine tools.

3. Electronics Technology: This includes microwave tubes, acoustic wave devices, flash discharge type X-ray systems, atomic frequency standards, waveform digitizers, and network analyzers.

4. Computer Technology: This includes high performance computing, signal and image processing, computer network technology, data

fusion, virtual prototyping, and computer-aided acquisition and logistics support.

5. Telecommunications Technology: This includes electromagnetic communications, cables and cable manufacturing, network management and control, and command, control, communications, and intelligence (C^3I) systems.

6. Sensors and Electronic Combat Technology: This includes optical sensors, cameras, marine, air, and space acoustic systems, magnetometers and magnetic gradiometers, and radar.

7. Navigation, Guidance, and Vehicle Control: This includes inertial navigation systems, gyroscopes, accelerometers, radio navigation and direction finding, map guidance systems, and flight control systems.

8. Marine Systems Technology: This includes advanced hull forms, submersible vehicles, (marine) power generation systems, and signature reduction.

9. Propulsion and Vehicular Systems Technology: This includes gas turbine propulsion systems, ramjet and scramjet combined cycle systems, aerospace structures and systems, rockets, and vehicle survivability.

10. Laser, Optics and Power Systems Technology: This includes gas, semiconductor, solid-state, and other lasers, optical mirrors, space qualified optical components, and power conditioning and pulsed power systems.

11. Directed Energy (DE) and Kinetic Energy (KE) Systems Technology: This includes high-energy laser systems, high power radio frequency systems, particle beam systems, and kinetic energy systems.

12. Munitions Devices and Energetic Materials Technology: This includes warhead, ammunition, payloads, gun propulsion, conventional

munitions survivability, tactical missile propulsion and integration, and energetic materials.

13. Chemical and Biological Systems Technology: This includes chemical warfare systems production facilities and processes, biopolymer production related to biological warfare capabilities, bio-derived materials, defensive systems.

14. Survivability and Hardening Technology: This includes underground nuclear weapons effects testing, pulsed-power driven nuclear weapons effects simulation sources, and nuclear effects on electromagnetic signal propagation.

15. Nuclear-Related Technology: This includes fissile materials enrichment, nuclear materials processing, fission reactor, nuclear weapons, and inertial confinement fusion.

The above subcategories are neither inclusive nor exclusive.

The Department of Defense, with input from the Intelligence Community, the military services, and industry representatives, assesses the R&D and manufacturing capabilities of other nations in these categories. Two enclosed tables depict the available assessments. In addition to visual comparisons of technological capabilities, the MCTL provides a brief summary of foreign capabilities in a given field.

The Foreign Technology Assessment Summary for Computer Technology, Table 5, reads:

> The Pacific Rim countries are a major source of personal computers including desk top, portable and lap top models; and some of these computers are more powerful than most installed western tactical military computers, although the Pacific Rim models may not meet military environmental and operating specifications. The Pacific Rim countries have acquired U.S. computer, microprocessor and integrated circuit

technology through licensing, joint development and purchase. The U.S. holds a world lead in microprocessor design and fabrication, and in key high performance computing technology areas (mainframes, computer networks, and parallel computing) and related software. The U.S. shares a lead in thin film heads and media for magnetic hard disk storage with Japan. It also shares a lead with Japan in the "development" and "production" of high performance computing.[1]

The Foreign Technology Assessment for Telecommunications Technology, Table 6, reads, in part:

All countries have some form of telecommunications for civil or military use. The "technology" which they possess in this area is dependent on whether they elected to produce equipment of their own design or rely on foreign purchases or licensing agreements....Cross-licensing arrangements or formations of consortia or joint ventures among the major manufacturers in various countries have resulted in "technology" transfers in many areas in both highly and lesser developed countries. Some of the lesser developed countries who had little or no installed equipment and were non-producers elected to participate in joint ventures to obtain modern equipment and "technology" and have moved ahead rapidly unhampered by obsolete inventories. South Korea and Taiwan are examples of these. While the Former Soviet Union (FSU) civil communication systems are predominantly analogue and limited in speed and capacity, they have produced effective communications systems for military purposes, especially naval. There are relatively few nations which have the capability of developing and manufacturing a successful communication satellite system exclusive of base stations. The U.S. is foremost in this ability and next in line is the FSU. They, in turn, are followed by France with the European nations. Others like the Japanese, have obtained their know-how from the U.S. or European nations.[2]

TABLE 5

COMPUTER TECHNOLOGY
FOREIGN TECHNOLOGY ASSESSMENT SUMMARY

Country	Digital Processing	Software	Hybrid Computing	Advanced Computing
Bulgaria	1	1	1	1
Canada	2	2	0	2
China	2	3	2	2
France	3	2	1	3
FSU	1	2	2	1
Germany	3	2	1	3
India	1	2	0	2
Israel	2	2	1	1
Japan	3	3	1	4
S. Korea	1	0	0	0
Netherlands	2	2	1	2
Taiwan	2	0	0	0
United Kingdom	3	3	1	3
United States	4	4	4	4

Source: Adapted from U.S. Department of Defense. Office of the Under Secretary of Defense for Acquisition. The Militarily Critical Technologies List (Alexandria: Institute for Defense Analyses, October 1992), 4-2.

Legend:
4--Capabilities in all critical elements.
3--Capabilities in majority of critical elements.
2--Capabilities in some critical elements.
1--Limited capability.
0--No capability or none identified.

FSU--Former Soviet Union

TABLE 6

TELECOMMUNICATIONS TECHNOLOGY
FOREIGN TECHNOLOGY ASSESSMENT SUMMARY

Country	Electro-magnetic	Cable	Switching	Networking	C^3
Brazil	3	2	2	1	0
Belgium	1	3	4	2	0
Canada	4	4	4	3	3
China	1	1	2	1	0
Egypt	0	1	0	0	0
France	4	4	4	4	3
FSU	3	1	1	1	1
Germany	4	4	4	4	3
Hong Kong	0	1	1	0	0
India	2	2	2	1	2
Iran	0	1	0	0	1
Iraq	0	1	0	0	1
Israel	3	2	2	2	4
Japan	4	4	4	3	3
N. Korea	0	1	0	0	0
S. Korea	3	3	3	3	3
Pakistan	0	1	0	0	0
Singapore	3	3	2	2	0
S. Africa	1	1	0	0	0
United Kingdom	4	4	4	4	3
United States	4	4	4	4	4

Source: Adapted from U.S. Department of Defense. Office of the Under Secretary of Defense for Acquisition. The Militarily Critical Technologies List (Alexandria: Institute for Defense Analyses, October 1992), 5-2.

Legend:
4--Capabilities in all critical elements.
3--Capabilities in majority of critical elements.
2--Capabilities in some critical elements.
1--Limited capability.
0--No capability or none identified.

C^3--Command, Control, and Communications
FSU--Former Soviet Union

APPENDIX C

GOVERNMENT DOCUMENTS AVAILABLE

The United States Government already makes some economic information published by intelligence agencies and agencies with economic reporting responsibilities available to the public. At present, the documents provide a broad overview of some subject areas and do not provide details about specific foreign companies. Anyone, to include foreign governments and companies, can purchase these documents, in either hard copy or CD/ROM form, from the National Technical Information Service (NTIS) or the Government Printing Office (GPO). NTIS listings are of publications available for years 1990 to 1993. GPO listings are of publications available from 1976 to 1993. Prices were not listed for most documents. A sample listing of available documents follows:

1. Title: Lithuania: An Economic Profile.

   Producer: Central Intelligence Agency.

   Available through: NTIS.

   Abstract: February 1993. Basic reference for assessing future development possibilities. Describes geography, population, and economy of Lithuania and compares its level of development, growth, and social welfare to that in Finland and Sweden. Equivalent reports are available on Latvia and Estonia.

2. Title: Trends in LDC External Debt, 1985-1991: A Reference Aid.

   Producer: Central Intelligence Agency.

Available through: NTIS.

Abstract: Provides recent data on the trends of Lesser Developed Countries (LDC) debt as compiled from World Bank, Organization for Economic Cooperation and Development (OECD), International Monetary Fund (IMF), and Bank for International Settlements sources. Data for 112 LDCs provided on aggregate LDC external debt, individual external debt positions, and IMF credit outstanding.

3. Title: Defense Industries of the Newly Independent States of Eurasia.

Producer: Central Intelligence Agency.

Available through: NTIS.

Abstract: January 1993. Overview of the defense-industrial base in each of the newly independent states of the former Soviet Union. Includes information on final assembly plants, component producers, material production facilities, and research, development, and test facilities.

4. Title: "Economic and Energy Indicators." (monthly publication)

Producer: Central Intelligence Agency.

Available through: NTIS.

Abstract: Information on industrial production, unemployment, consumer price inflation, exchange rate trends, foreign trade and trade prices, petroleum consumption, petroleum production, and petroleum imports for the Big Seven industrial nations (United States, Japan, Germany, France, United Kingdom, Italy, and Canada).

5. Title: Japan: Ministry of International Trade and Industry (MITI).

Producer: Central Intelligence Agency.

Available through: NTIS.

Abstract: September 1991. Organizational structure of MITI with photographs and brief biographies of the minister, vice ministers, and director generals.

6. Title: OECD Trade with Mexico and Central America.

Producer: Central Intelligence Agency.

Available through: NTIS.

Abstract: February 1992. Commodity statistics of Organization for Economic Cooperation and Development (OECD) trade with Mexico and Central America.

7. Title: EC 1992: A Commerce Department Analysis of European Community Directives.

Producer: Department of Commerce.

Available through: GPO, $13.00.

Abstract: March 1990. Outlines industrial laws and regulations in the European Economic Community countries.

8. Title: The Market for Health Care Equipment, Indonesia.

Producer: Department of Commerce.

Available through: GPO.

Abstract: May 1977, updated May 1982. A survey of medical equipment requirements and medical business opportunities in Indonesia.

9. Title: Foreign Economic Trends and their Implications for the United States.

Producer: Department of Commerce.

Available through: GPO, $90.00.

Abstract: January 1979, updated September 1973. No abstract listed in GPO database.

10. Title: Economic Growth of OECD Countries.

Producer: Department of State. Bureau of Intelligence and Research.

Available through: GPO.

Abstract: July 1982. Special report on the economic status of OECD nations covering the period 1970 to 1980.

11. Title: Indicators of Comparative East-West Economic Strength.

Producer: Department of State. Bureau of Intelligence and Research.

Available through: GPO.

Abstract: March 1978. Statistical comparison with tables and charts of economic indicators between Western nations (U.S. and Europe) and Eastern nations (East Europe and USSR).

A review of the database for GPO documents available shows that the majority of Department of Treasury documents deal with U.S. treasury bonds, government notes, and U.S. Government appropriations. Department of Commerce listings deal most often with air pollution controls, small business and minority opportunities, and publications on U.S. industries intended for foreign distribution. Most of the Department of State documents are concerned with territorial waters, maritime boundaries, continental shelf boundaries, border demarcations, and security information for Americans traveling overseas. Central Intelligence Agency documents are available through NTIS; they were the most specific business, industry, and economic related documents from a review of documents in both the GPO and NTIS databases. This sample listing was taken from a review of 793 titles and abstracts.

APPENDIX D

LITERATURE REVIEW

Many articles and some books exist that discuss economic competitiveness and the pluses and minuses of intelligence support to U.S. corporations. Academia and business have increased their interest in the topic during the past ten years; in the past three years Congress and Presidents Bush and Clinton have publicly stated an interest in U.S. economic competitiveness. Congress conducted a hearing on economic espionage and the provision of government intelligence to private industry in 1992. American businesses also expressed concern with and identified U.S. competitiveness shortcomings and challenges. Some companies commissioned studies from private research corporations to describe the problem and recommend solutions. Some business and consulting officials (many of them former USG intelligence agency employees) have written articles advising U.S. companies on how to improve internal security to prevent information theft.

Several former Directors of Central Intelligence (DCI) have spoken and written openly about the appropriateness and ability of the U.S. Intelligence Community, particularly the Central Intelligence Agency, to collect, analyze, and provide intelligence on competitors and markets to U.S. companies. Also, members of the Senate Select Committee on Intelligence (SSCI) and House Permanent Select Committee on Intelligence (HPSCI) have published their views on the subject. These individuals all have years of

experience working in or with the Intelligence Community; they are knowledgeable on the capabilities, strengths, and weaknesses of the IC.

Congressmen who advocate IC support to competitive, or economic, intelligence include: David L. Boren (Senate, D-OK, SSCI)[1], Dave McCurdy (House, D-OK, HPSCI)[2], and Dennis DeConcini (Senate, D-AZ, SSCI).[3] Former Directors of Central Intelligence who agree are Stansfield Turner[4] and Richard Helms.[5] Former DCI Robert Gates[6] and the current DCI James Woolsey[7]do not support the concept of giving government intelligence to companies.

These individuals, and others, raise interesting and complex questions with respect to spying on allies for economic not military information and the ability of the Intelligence Community to provide relevant and timely economic intelligence to anyone. Some authors suggest that companies can access sufficient information from open source databases. Other authors argue that corporations in foreign countries are not directed (or hampered) by law to make detailed corporate information available publicly as are U.S. corporations. Therefore, in their view, the necessary information on competitors is not publicly available in open source databases and the IC would be needed to fill this information gap.

A serious shortcoming of most of the available material is that the authors routinely recommend only a "yes" or "no" to the proposal that the IC provide intelligence to U.S. corporations. The writers do not discuss in adequate detail the rationale for their recommendations and do not offer alternate solutions to the problem. They also do not discuss, in any depth, the USG's current role in and capabilities to provide economic intelligence.

Although many concerned individuals have addressed the issue, the majority of the available material deals superficially with the topic.

Some sources center on in-depth descriptions of how foreign competitors employ economic espionage or buy key U.S. companies to steal U.S. technologies and markets. Peter Schweizer's Friendly Spies: How America's Allies are Using Economic Espionage to Steal Our Secrets discusses the economic intelligence activities conducted against the United States by Japan, Israel, South Korea, and France. Schweizer's book contains the most current information available on foreign economic espionage activities directed against the United States. His sources include senior CIA, NSA, and FBI officials who he interviewed to get material for the book. Although he does not name most of his interviewees, they gave him access to information that was previously classified and not available in other published sources.

Martin and Susan J. Tolchin's Selling Our Security: The Erosion of America's Assets provides a comprehensive background on how the United States lost its world dominance in several critical high-level technologies such as semi-conductor and optical lens manufacturing. They discuss: how foreign companies have legally acquired controlling shares of U.S. based high-technology companies; how the foreign companies then transfer patents and manufacturing abilities to their home base in effect stripping the American company of its knowledge and competitive ability; the lack of a definition to determine what a "U.S." company is; and the lack of policy direction from past presidential administrations to address the foreign threat to U.S. competitiveness and industrial knowledge.

Alexandre de Marenches headed the French intelligence agency, the Direction General de la Securite Exterieure (DGSE) from 1970 to 1981. He has written two books about his experiences: Dans le Secret des Princes (1986), not available in English, and The Fourth World War: Diplomacy and Espionage in the Age of Terrorism (1992). The Fourth World War repeats some of the material found in the first book.

In both books, de Marenches candidly discusses the importance of economic espionage to France's national security. He describes collection methods and industrial targets of the French intelligence service. De Marenches recounts how France deliberately targeted the United States for financial and technological information. Described espionage operations took place predominantly in France; de Marenches does not detail oversees espionage activities, probably due to political sensitivities. In an interesting twist, after he describes French economic espionage activities against the United States, he then writes about Japanese economic spy activities directed against France. He compliments the Japanese as being experts in industrial espionage.

A study published by the American Institute for Business Research, Protecting Corporate America's Secrets in the Global Economy: A Risk Analysis of the New Threats to U.S. Business Information, describes the U.S. economic competitiveness problem and proposes several recommendations to assist businesses in reducing their risk to become victims to economic espionage. While well-written, the study does not contain a bibliography and does not name the authors.

Alvin Toffler provides an interesting perspective on where he believes business, global competitiveness, and intelligence are headed in the

21st century. In Powershift, he describes global information wars, already underway, that are redefining power and shifting who holds power worldwide. Competitive intelligence and government intelligence play major roles in the work. He briefly discusses the strengths and weaknesses of industry and government intelligence organizations in the area of economic intelligence. Toffler predicts that private industry's competitive intelligence efforts will eventually merge with government intelligence as nations will no longer be able to separate their security from their economic strength. This, in fact, is the argument that the government and former intelligence officials listed above use to promote the concept.

Several books outline the history and basic collection and analytical assets of the Intelligence Community. Although much information about the American intelligence apparatus is classified, the authors have pieced together data from unclassified sources. Some authors, in fact, are former employees of government intelligence agencies. As mentioned earlier, information contained in the books on the internal organization of some agencies, particularly the CIA, DIA, and NSA , is now outdated. These agencies have been reorganizing, changing their line-and-block charts, throughout 1992 and 1993. Despite this, the core information contained in these books regarding missions assigned to the agencies remains accurate.

Comprehensive descriptions of the Intelligence Community are contained in: The U.S. Intelligence Community: Foreign Policy and Domestic Activities by Lyman B. Kirkpatrick, Jr. (a former senior CIA employee); The U.S. Intelligence Community by Jeffrey T. Richelson; and Silent Warfare: Understanding the World of Intelligence by Abram N. Shulsky (a former consultant on the President's Foreign Intelligence Advisory Board). Deep

Black by William Burrows gives a detailed look at the capabilities of and the uses of the information provided by satellite and aircraft reconnaissance systems.

Three former USG officials, Amos A. Jordan, Lawrence J. Korb, and William J. Taylor, Jr., wrote American National Security: Policy and Process. It is a basic and integrated textbook on U.S. national security. Jordan, Korb, and Taylor cover the role of military, economic, and diplomatic elements of power, the national policy and decision-makers (the President, National Security Council, Congress, and the Department of Defense), issues of national concern (nuclear proliferation, peacekeeping operations, limited war, the economy), and strategic concerns in regions of the world.

Three chapters contain information used in this thesis: Chapter 7, "Intelligence and National Security," Chapter 14, "Economic Challenges to National Security," and Chapter 24, "National Security Perspectives for the 1990's." Information in these chapters ties together the importance of economic strength to national security, the economic challenges to be met in the future, and the ability of the Intelligence Community to support national decision-makers.

The study by Richard Best, Jr., The U.S. Intelligence Community Role in Supporting Economic Competitiveness, discusses the issue in greater detail than the other works cited in the bibliography. Commissioned by Congress and published in 1990, the report is a concise (38 page) summary of the competitiveness problem, lists intelligence products on economic subjects currently available for public use, and discusses the pros and cons of increased government intelligence support to business. Best ends the study with possible implementation options if a decision is made to task the IC to

provide more economic information to the public and business. The implementation options are broad and superficial; the report does not contain a final recommendation on whether or not the USG should provide economic intelligence to the business community.

Clyde V. Prestowitz worked as an expert in Japanese trade negotiations for the U.S. Department of Commerce from 1983 to 1986. In his book, Trading Places: How We Are Giving Our Future to Japan and How to Reclaim It, he recounts his tour at Commerce and his dealings with the Japanese. Prestowitz documents U.S. and Japanese trade relations from post-World War II to 1988. He provides insights to Japan's cultural approach to conducting business, discusses Japan's take-over of industries that had been U.S. dominated (semi-conductors and machine tools), and describes the Japanese government and business bureaucracy.

Prestowitz also discusses how he feels U.S. trade laws hamper U.S. industry's ability to remain internationally competitive and describes the U.S. players in the international economic business (Departments of Defense, Treasury, Commerce, and State; the National Security Council; and the CIA). Since he reads Japanese, Prestowitz is able to quote Japanese literature, not available in English, describing Japanese businessmen's views toward the U.S. as an economic competitor and their economic goals.

Japan: 2000 is a report on Japan's strategic economic ethic goals and business ethic; it was prepared by the Rochester Institute of Technology and commissioned by the CIA. Its author, Andrew Dougherty describes the Japanese paradigm of business: there are no rules, no absolute principles; consists of powerful industry groups that exclude undesirables--all foreigners and Japanese who do not conform to mainstream expectations; is anti-

American and anti-European; and rests on Japanese ultra-nationalism and self-proclaimed racial supremacy.[8]

The brief report, 47 pages, outlines how the U.S. lost economic ground to Japan through its use of U.S. cultural, legal, and political weaknesses to its advantage. It provides a blueprint for what Japan wants economically, how it has targeted U.S. business and government to achieve world economic and technological supremacy, and how it will achieve its goals. Dougherty briefly discusses U.S. business shortcomings and what must be done to overcome them and regain the international economic lead from Japan. Shortly after its release in 1991, some Americans criticized Japan: 2000 as being racist and self-serving--that the CIA was looking for a new threat to replace the then dying Soviet Union.[9]

ENDNOTES

Chapter 1

[1]Susumu Awanohara and Melana Zyla, "Spooks for Industry," Far Eastern Economic Review, 25 February 1993, 15.

[2]American Institute for Business Research, Protecting Corporate America's Secrets in the Global Economy (Framington: American Institute for Business Research, 1993), 22.

[3]David L. Boren, "The Winds of Change at the CIA," The Yale Law Journal, January 1992, 861-862.

[4]National Academy of Engineering, National Interests in an Age of Global Technology (Washington, D.C.: National Academy Press, 1991), 17.

[5]Council on Competitiveness, Gaining New Ground: Technology Priorities for America's Future (Washington, D.C.: Council on Competitiveness, March 1991), 1.

[6]Daniel F. Burton and B.R. Inman, "Technology and Competitiveness: The New Policy Frontier," Foreign Affairs, Spring 1990, 119.

[7]Ibid., 117-118.

[8]National Science Board, Science & Engineering Indicators-1991 (Washington, D.C.: U.S. Government Printing Office, 1991), 136, 402.

[9]Amos A. Jordan, Lawrence J. Korb, and William J. Taylor, Jr., American National Security: Policy and Process (Baltimore: The Johns Hopkins University Press, 1993), 287.

[10]American Institute for Business Research, Protecting Corporate America's Secrets in the Global Economy (Framington: American Institute for Business Research, 1993), 33.

[11]Ibid., 33.

[12]Ibid., 34.

[13]Ibid., 23

[14]Ibid., 23

[15]Peter Schweizer, Friendly Spies (New York: Atlantic Monthly Press, 1993), 236-237.

[16]Ibid., 71.

[17]Ibid., 187-198.

[18]George Bush, National Security Strategy of the United States (Washington, D.C.: The White House, January 1993), 9.

[19]U.S. Department of Defense, National Military Strategy of the United States (Washington, D.C.: Department of Defense, January 1992), 10.

[20]U.S. Department of Defense. Office of the Under Secretary of Defense for Acquisition. Bolstering Defense Industrial Competitiveness (Washington, D.C.: Office of the Under Secretary of Defense, July 1988), v.

[21]Ibid., v.

[22]Jordan, Korb, Taylor, Jr., 285.

[23]Ronald Reagan, "Executive Order No. 12333," Federal Register (Washington, D.C.: U.S. Government Printing Office, 8 December 1991), 59943.

Chapter 3

[1]U.S. Congress. House. Committee on the Judiciary. Subcommittee on Economic and Commercial Law. The Threat of Foreign Economic Espionage to U.S. Corporations (Washington, D.C.: U.S. Government Printing Office, 1992), 53.

[2]Ibid., 54.

[3]Ibid., 53.

[4]American Institute for Business Research, Protecting Corporate America's Secrets in the Global Economy (Framington: American Institute for Business Research, 1993) 37.

[5]Peter Schweizer, Friendly Spies (New York: Atlantic Monthly Press, 1993), 7.

[6]American Institute for Business Research, 40.

[7]Schweizer, 99.

[8]American Institute for Business Research, 37.

[9]Ibid., 42; and Schweizer, 103.

[10]Schweizer, 99, 103, 110, 112-113.

[11]Ibid., 113.

[12]Ibid., 124-126.

[13]American Institute for Business Research, 136.

[14]U.S. Congress. House. Committee on the Judiciary, 125.

[15]Ibid., 122.

[16]American Institute for Business Research, 42-43.

[17]Bill Gertz, "French Probed as Spies Against U.S. Corporations," Washington Times, 4 June 1993.

[18]Alexandre de Marenches and Christine Ockrent, Dans le Secret des Princes (Paris: Editions Stock, 1986), 131.

[19]Alexandre de Marenches and David A. Andelman. The Fourth World War: Diplomacy and Espionage in the Age of Terrorism (New York: William and Morrow and Company, Inc., 1992), 115.

[20]Ibid., 115.

[21]Dennis DeConcini, Robert Gates, and Larry Watson, "Spy Stories" (Interview by Consuelo Mack: "Wall Street Journal Report on Television," 8 August 1993, Journal Graphics, transcript 567), 5.

[22]Clyde V. Prestowitz, Trading Places: How We Are Giving Our Future to Japan and How to Reclaim It (New York: Basic Publishers, Inc., 1988), 1.

[23]Ibid., 1.

[24]Ibid., 2.

[25]Schweizer, 80.

[26]Andrew J. Dougherty, Japan: 2000 (Rochester: Rochester Institute of Technology, 11 February 1991), 25.

[27]Schweizer, 71.

[28]de Marenches and Andelman. The Fourth World War, 116.

[29]Ibid., 117.

[30]Ibid., 117.

[31]Ibid., 117.

[32]Ibid., 117.

[33]Schweizer, 86.

[34]U.S. Congress. House. Committee on the Judiciary, 19.

[35]Martin and Susan J. Tolchin, Selling our Security: The Erosion of America's Assets (New York: Alfred A. Knopf, 1992), 72-75.

[36]Ibid., 98-105.

[37]Prestowitz, 50.

[38]Ibid., 50.

[39]Ibid., 50.

[40]Ibid., 50.

[41]Ibid., 56.

[42]Martin and Susan J. Tolchin, 87.

[43]Ibid., 92.

[44]Ibid., 88-91, and Prestowitz, 8-58.

[45]Martin and Susan J. Tolchin, 350

[46]Schweizer, 78.

[47]Ibid., 83.

[48]B.R. Inman and Daniel F. Burton, Jr., "Technology and Competitiveness: The New Policy Frontier," Foreign Affairs, Spring 1990, 119.

[49]Schweizer, 85.

[50]bid., 82.

[51]Ibid., 82.

Chapter 4

[1]Amos A. Jordan, Lawrence J. Korb, and William J. Taylor, Jr., American National Security: Policy and Process (Baltimore: The Johns Hopkins University Press, 1993), 140.

[2]Larry Grossman, "Intelligence in a World of Change," Government Executive, March 1992, 12.

[3]Jeffrey T. Richelson, The U.S. Intelligence Community (Cambridge: Ballinger Publishing Company, 1989), 295.

[4]Richelson, 16-17.

[5]Grossman, 14.

[6]Robert Gates, "Spy Stores" (Interview by Consuelo Mack: "Wall Street Journal Report on Television," 8 August 1993, Journal Graphics, transcript 567), 7.

[7]James Woolsey, "Future of Intelligence Issues" (Speech given to the Executives' Club of Chicago, Broadcast on C-SPAN, 24 November 1993).

[8]Richelson, 36.

[9]Ronald Reagan, "Executive Order 12333," Federal Register (Washington, D.C.: U.S. Government Printing Office, 8 December 1981), 59946.

[10]Richelson, 8, 40.

[11]U.S. Department of Defense, Joint Strategy Review Plan Key Judgment Paper: Technology Proliferaion and U.S. Technological Superiority (Washington, D.C.: Defense Intelligence Agency, 13 April 1993), 11.

[12]Ibid., 5.

[13]U.S. Department of Defense, 6.

[14]Ibid., 12.

[15]Gerald W. Hopple and Bruce W. Watson, editors, The Military Intelligence Community (Boulder: Westview Press, 1986), 62.

[16]Reagan, 59950.

[17]U.S. Department of Defense. Office of the Chairman. The Joint Chiefs of Staff, JCS Pub 1-02: Department of Defense Dictionary of Military and Associated Terms (Washington, D.C.: U.S. Government Printing Office, 1 December 1989), 80.

[18]Grossman, 13.

[19]Peter Schweizer, Friendly Spies (New York: Atlantic Monthly Press, 1993), 291.

[20]Richelson, 127.

[21]Ibid., 129.

[22]Jordan, Korb, and Taylor, Jr., 146.

[23]Richelson, 132.

[24]Stephen Barlas, "Does CIA Have a Role in Foreign Market Research?" Marketing News, 7 January 1991, 5.

[25]U.S. Department of Defense. Office of the Under Secretary of Defense for Acquisition (International Policy), Technology Identification and Analyses Center FY 1991 and FY 1992 Report (Alexandria: Institute for Defense Analyses, January 1993), VI-1.

[26]Ibid., III-4.

Chapter 5

[1]Abram N. Shulsky, Silent Warfare: Understanding the World of Intelligence (Washington, D.C.: Brassey's (U.S.), Inc., 1991), 17.

[2]Alexandre de Marenches and David A. Andelman. The Fourth World War: Diplomacy and Espionage in the Age of Terrorism (New York: William Morrow and Company, Inc., 1992), 251.

[3]Jeffrey T. Richelson. The U.S. Intelligence Community (Cambridge: Ballinger Publishing Company, 1989), 187.

[4]Gerald W. Hopple and Bruce W. Watson, editors, The Military Intelligence Community (Boulder: Westview Press, 1986), 47.

[5]Richard F. Janssen, "Rent-a-Spook," International Business, June 1993, 75.

[6]Schulsky, 23-24.

[7]Richelson, 150-151, 155.

[8]Ibid., 150-152.

[9]Ibid., 153.

[10]Ibid., 153.

[11]Larry Grossman, "Intelligence in a World of Change," Government Executive, March 1992, 12.

[12]Peter Schweizer. Friendly Spies (New York: Atlantic Monthly Press, 1993), 93.

[13]Kenneth F. Englade, "Competitor Intelligence Comes in from the Cold," Across the Board, April 1989, 22-23.

[14]Ibid., 22-23.

[15]Kate Bertrand, "The Global Spyglass," Business Marketing, September 1990, 53.

[16]Richard A. Best, Jr. The U.S. Intelligence Community: A Role in Supporting Economic Competitiveness (Washington, D.C.: Congressional Research Service, 7 December 1990), 15.

[17]Amos A. Jordan, Lawrence J. Korb. and William J. Taylor, Jr., American National Security: Policy and Process (Baltimore: The Johns Hopkins University Press, 1993), 156.

[18]Stansfield Turner. "What Is the Role of the CIA in the '90s?" (Interview by Larry King, "Larry King Live," 5 August 1992, Journal Graphics, transcript 621), 5.

[19]Amy Borrus. "Should the CIA Start Spying for Corporate America?" Business Week, 14 October 1991, 100.

[20]Clyde V. Prestowitz, Trading Places: How We Are Giving Our Future to Japan and How to Reclaim It (New York: Basic Books, Inc., 1988), 446-447.

[21]Turner, (Interview by Larry King, transcript 621), 7.

[22]Borrus, 100.

[23]Schweizer, 285.

[24]James Woolsey. "Inside the CIA," (Interview by Larry King, "Larry King Live," 30 November 1993, Journal Graphics, transcript 979), 6.

[25]Turner, (Interview by Larry King, transcript 621), 6.

[26]Grossman, 13.

[27]Woolsey, 6.

[28]U.S. Congress. House. Committee on the Judiciary. Subcommittee on Economic and Commercial Law. The Threat of Foreign Economic Espionage to U.S. Corporations (Washington, D.C.: U.S. Government Printing Office, 1992), 5.

[29]Jordan,Korb and Taylor, Jr., 158.

[30]Schweizer, 90-91.

[31]Best, 5.

[32]Stephen Barlas, "Does CIA Have a Role in Foreign Market Research?" Marketing News, 7 January 1991, 5.

[33]Schweizer, 301-302.

[34]Ibid., 301-302.

[35]Ibid., 301-302.

[36]James Woolsey, "Intelligence Gathering and International Relations" (Speech given to the American Bar Association, Broadcast on C-SPAN, 29 April 1994).

[37]Janssen, 75.

Chapter 6

[1]Robert Gates, "Why Spy?" (Interview by Adam Smith, "Adam Smith's Money World," 23 April 1993, Journal Graphics, transcript 921), 3.

[2]Peter Schweizer. Friendly Spies (New York: Atlantic Monthly Press, 1993), 296.

[3]Gates, 3.

Appendix A

[1]U.S. Department of Defense. Office of the Chairman. The Joint Chiefs of Staff, JCS Pub 1-02: Department of Defense Dictionary of Military and Associated Terms (Washington, D.C.: U.S. Government Printing Office, 1 December 1989), 80.

[2]U.S. Congress. House. Committee on the Judiciary. Subcommittee on Economic and Commercial Law, The Threat of Foreign Economic Espionage to U.S. Corporations (Washington, D.C.: U.S. Government Printing Office, 1992), 29.

[3]U.S. Department of Defense. Office of the Chairman. The Joint Chiefs of Staff, 171.

[4]Ibid., 174.

[5]Defense Intelligence College, Glossary of Intelligence Terms (Washington, D.C.: Defense Intelligence College, undated), 8.

[6]William R. Corson, The Armies of Ignorance (New York: The Dial Press, 1977), 78.

[7]U.S. Department of Defense. Office of the Under Secretary of Defense for Acquisition, The Militarily Critical Technologies List (Alexandria: Institute for Defense Analyses, October 1992), 2.

[8]Ibid., ix-xiv.

[9]American Institute for Business Research, Protecting Corporate America's Secrets in the Global Economy (Framington: American Institute for Business Research, 1993), 42.

[10]U.S. Department of Defense. Office of the Chairman. The Joint Chiefs of Staff, 262.

Appendix B

[1]U.S. Department of Defense. Office of the Under Secretary of Defense for Acquisition, The Militarily Critical Technologies List (Alexandria: Institute for Defense Analyses, October 1992), 4-3.

[2]Ibid., 5-3.

Appendix D

[1]Susumu Awanohara. "Paradigm Paranoia: CIA Report Warns of Japanese Economic Domination," Far Eastern Economic Review, 27 June 1991, 15.

[2]Larry Grossman. "Intelligence in a World of Change," Government Executive, March 1992, 14.

[3]Dennis DeConcini. "Why Spy?" Interview by Adam Smith ("Adam Smith's Money World," 23 April 1993). Journal Graphics, transcript 921, 2; and Dennis DeConcini. "Spy Stories," Interview by Consuelo Mack ("The Wall Street Journal Report on Television," 8 August 1993). Journal Graphics, transcript 567, 6.

[4]Stansfield Turner. "What Is the Role of the CIA in the '90s?" Interview by Larry King ("Larry King Live," 5 August 1992). Journal Graphics, transcript 621, 2-9.

[5]Michael J. Stedman. "Industrial Espionage: What You Don't Know Can Hurt You," Business and Society Review, Winter 1991, 29.

[6]U.S. Congress. House. Committee on the Judiciary. Subcommittee on Economic and Commercial Law, The Threat of Foreign Economic Espionage to U.S. Corporations (Washington, D.C.: U.S. Government Printing Office, 1992), 53; and Robert Gates. "Spy Stories," Interview by Consuelo Mack ("The Wall Street Journal Report on Television," 8 August 1993). Journal Graphics, transcript 567, 3.

[7]James Woolsey. "Inside the CIA," Interview by Larry King ("Larry King Live," 30 November 1993). Journal Graphics, transcript 979, 6.

[8]Andrew J. Dougherty. Japan: 2000 (Rochester: Rochester Institute of Technology, 11 February 1991), 14-20.

[9]Awanohara, 15.

BIBLIOGRAPHY

Books

Burrows, William E. Deep Black: Space Espionage and National Security. New York: Random House, 1986.

Corson, William R. The Armies of Ignorance: The Rise of the American Intelligence Empire. New York: The Dial Press, 1977.

de Marenches, Alexandre, and David A. Andelman. The Fourth World War: Diplomacy and Espionage in the Age of Terrorism. New York: William Morrow and Company, Inc., 1992.

de Marenches, Alexandre, and Christine Ockrent. Dans le Secret des Princes. Paris: Editions Stock, 1986.

Hillway, Tyrus. Introduction to Research. Boston: Houghton Mifflin Company, 1964.

Hopple, Gerald W., and Bruce W. Watson, editors. The Military Intelligence Community. Boulder: Westview Press, 1986.

Jordan, Ames A., Lawrence J. Korb, and William J. Taylor, Jr. American National Security: Policy and Process. Baltimore and London: The Johns Hopkins University Press, 1993.

Kirkpatrick, Jr., Lyman B. The U.S. Intelligence Community: Foreign Policy and Domestic Activities. New York: Hill and Wang, 1973.

Prestowitz, Jr., Clyde V. Trading Places: How We Are Giving Our Future to Japan and How to Reclaim It. New York: Basic Books, Inc., 1988.

Richelson, Jeffrey T. The U.S. Intelligence Community. Cambridge: Ballinger Publishing Company, 1989.

Schweizer, Peter. Friendly Spies: How America's Allies are Using Economic Espionage to Steal Our Secrets. New York: Atlantic Monthly Press, 1993.

Shulsky, Abram N. Silent Warfare: Understanding the World of Intelligence. Washington, D.C.: Brassey's (US), Inc., 1991.
Toffler, Alvin. Powershift. New York: Bantam Books, 1990.

Tolchin, Martin, and Susan J. Tolchin. Selling our Security: The Erosion of America's Assets. New York: Alfred A. Knopf, 1992.

Periodicals and Articles

Arbetter, Lisa. "Identity Crisis," Security Management, April 1993, 11.

Awanohara, Susumu. "Paradigm Paranoia: CIA Report Warns of Japanese Economic Domination," Far Eastern Economic Review, 27 June 1991, 15.

Awanohara, Susumu, and Melana Zyla. "Spooks for Industry," Far Eastern Economic Review, 25 February 1993, 15.

Barlas, Stephen. "Does CIA Have a Role in Foreign Market Research?" Marketing News, 7 January 1991, 2,5.

Bertrand, Kate. "The Global Spyglass," Business Marketing, September 1990, 52-53.

Boren, David L. "The Winds of Change at the CIA." The Yale Law Journal, January 1992, 853-865.

Borrus, Amy. "Should the CIA Start Spying for Corporate America?" Business Week, 14 October 1991, 96-100.

Borrus, Amy. "Why Pinstripes Don't Suit the Cloak-and-Dagger Crowd," Business Week, 17 May 1993, 39.

Englade, Kenneth F. "Competitor Intelligence Comes in from the Cold," Across the Board, April 1989, 18-25.

Gates, Robert. "The Future of American Intelligence," Vital Speeches of the Day, 1 January 1992, 171-74.

Gertz, Bill. "French Probed as Spies Against U.S. Companies," Washington Times, 4 June 1993.

Grossman, Larry. "Intelligence in a World of Change," Government Executive, March 1992, 11-16.

Inman, B. R., and Daniel F. Burton, Jr. "Technology and Competitiveness:

The New Policy Frontier," Foreign Affairs, Spring 1990, 116-134.

Janssen, Richard F. "Rent-a-Spook," International Business, June 1993, 75-76.

Sookdeo, Ricardo. "Jobless? The CIA is Hiring Now," Fortune, 19 April 1993, 16.

Stedman, Michael J. "Industrial Espionage: What You Don't Know Can Hurt You," Business and Society Review, Winter 1991, 25-32.

Turner, Stansfield. "Intelligence for a New World Order," Foreign Affairs, Fall 1990, 150-66.

Government Documents

Best, Richard A., Jr. The U.S. Intelligence Community: A Role in Supporting Economic Competitiveness. Washington, D.C.: Congressional Research Service, 7 December 1990.

Bush, George. National Security Strategy of the United States. Washington, D.C.: The White House, January 1993.

Council on Competitiveness. Gaining New Ground: Technology Priorities for America's Future. Washington, D.C.: U.S. Government Printing Office, 1991.

Defense Intelligence College. Glossary of Intelligence Terms. Washington, D.C.: Defense Intelligence College, n.d.

National Academy of Engineering. National Interests in an Age of Global Technology. Washington, D.C.: National Academy of Engineering, 1991.

National Science Board. Science & Engineering Indicators-1989. Washington, D.C.: U.S. Government Printing Office, 1989.

National Science Board. Science & Engineering Indicators-1991. Washington, D.C.: U.S. Government Printing Office, 1991.

Reagan, Ronald. "Executive Order No. 12333," Federal Register, 8 December 1981, 59942-56.

U.S. Congress. House. Committee on the Judiciary. Subcommittee on Economic and Commercial Law. The Threat of Foreign Economic

Espionage to U.S. Corporations. 102nd Cong., 2nd sess., 29 April and 7 May 1992.

U.S. Department of Defense. Office of the Chairman. The Joint Chiefs of Staff. JCS Pub 1-02: Department of Defense Dictionary of Military and Associated Terms. Washington, D.C.: U.S. Government Printing Office, 1 December 1989.

U.S. Department of Defense. Office of the Under Secretary of Defense for Acquisition. Bolstering Defense Industrial Competitiveness. Washington, D.C.: Office of the Secretary of Defense, July 1988.

U.S. Department of Defense. Office of the Under Secretary of Defense for Acquisition. The Militarily Critical Technologies List. Alexandria: Institute for Defense Analyses, October 1992.

U.S. Department of Defense. Office of the Under Secretary of Defense for Acquisition (International Programs). Technology Identification and Analyses Center FY 1991 and FY 1992 Report. Alexandria: Institute for Defense Analyses, January 1993.

U.S. Department of Defense. National Military Strategy of the United States. Washington, D.C.: Department of Defense, January 1992.

U.S. Department of Defense. Joint Strategy Review Plan Key Judgment Paper: Technology Proliferation and U.S. Technological Superiority. Washington, D.C.: Defense Intelligence Agency, 13 April 1993.

Interviews

DeConcini, Dennis, Robert Gates, Daniel Moynihan, and Stansfield Turner. "Why Spy?" Interview by Adam Smith ("Adam Smith's Money World," 23 April 1993). Journal Graphics, transcript 921.

DeConcini, Dennis, Robert Gates, and Larry Watson. "Spy Stories." Interview by Consuelo Mack ("The Wall Street Journal Report on Television," 8 August 1993). Journal Graphics, transcript 567.

Turner, Stansfield. "What Is the Role of the CIA in the '90s?" Interview by Larry King ("Larry King Live," 5 August 1992). Journal Graphics, transcript 621.

Woolsey, James. "Inside the CIA." Interview by Larry King ("Larry King Live," 30 November 1993). Journal Graphics, transcript 979.

Other Sources

American Institute for Business Research. Protecting Corporate America's Secrets in the Global Economy. Framingham: American Institute for Business Research, 1993.

Dougherty, Andrew J. Japan: 2000. Rochester: Rochester Institute of Technology, 11 February 1991.

Woolsey, James. "Future of Intelligence Issues." Speech given to the Executives' Club of Chicago. Broadcast on C-SPAN, 24 November 1993.

Woolsey, James. "Intelligence Gathering and International Relations." Speech given to the American Bar Association, Washington, D.C. Broadcast on C-SPAN, 29 April 1994.

INITIAL DISTRIBUTION LIST

1. Combined Arms Research Library
   U.S. Army Command and General Staff College
   Fort Leavenworth, KS 66027-6900

2. Defense Intelligence Agency
   Mr. Peter K. Raimondi
   PAN-1 (DIAC)
   Washington, D.C. 20340

3. Defense Technical Information Center
   Cameron Station
   Alexandria, VA 22314

4. MAJ Cyrus E. Holliday
   CAC Threats
   Fort Leavenworth, KS 66027

5. LTC Nancy Morales
   CTAC
   USACGSC
   Fort Leavenworth, KS 66027-6900

6. LTC Thomas K. Adams
   DJCO
   USACGSC
   Fort Leavenworth, KS 66027-6900

7. COL Robert W. Duffner
   7608 Pickard N.E.
   Albuquerque, NM 87110

CERTIFICATION FOR MMAS DISTRIBUTION STATEMENT

1. Certification Date: 05/05/94

2. Thesis Author: Eric G. Powell

3. Thesis Title: The Capabilities of the U.S. Government to Collect and Analyze Economic Intelligence

4. Thesis Committee Members Signatures: Lynn S. Dollisky MAJ, MI
Nancy A. Morales, LTC, MI
LTC MI

5. Distribution Statement: See distribution statements A-X on reverse, then circle appropriate distribution statement letter code below:

(A) B C D E F X SEE EXPLANATION OF CODES ON REVERSE

If your thesis does not fit into any of the above categories or is classified, you must coordinate with the classified section at CARL.

6. Justification: Justification is required for any distribution other than described in Distribution Statement A. All or part of a thesis may justify distribution limitation. See limitation justification statements 1-10 on reverse, then list, below, the statement(s) that applies (apply) to your thesis and corresponding chapters/sections and pages. Follow sample format shown below:

S	SAMPLE	SAMPLE	SAMPLE	S
A	Limitation Justification Statement	/ Chapter/Section	/ Page(s)	A
M				M
P	Direct Military Support (10)	/ Chapter 3	/ 12	P
L	Critical Technology (3)	/ Sect. 4	/ 31	L
E	Administrative Operational Use (7)	/ Chapter 2	/ 13-32	E
	SAMPLE	SAMPLE	SAMPLE	

Fill in limitation justification for your thesis below:

Limitation Justification Statement	/ Chapter/Section	/ Page(s)
	/	/
	/	/
	/	/
	/	/
	/	/

7. MMAS Thesis Author's Signature: Eric G. Powell

STATEMENT A: Approved for public release; distribution is unlimited. (Documents with this statement may be made available or sold to the general public and foreign nationals).

STATEMENT B: Distribution authorized to U.S. Government agencies only (insert reason and date ON REVERSE OF THIS FORM). Currently used reasons for imposing this statement include the following:

X 1. Foreign Government Information. Protection of foreign information.

X 2. Proprietary Information. Protection of proprietary information not owned by the U.S. Government.

X 3. Critical Technology. Protection and control of critical technology including technical data with potential military application.

X 4. Test and Evaluation. Protection of test and evaluation of commercial production or military hardware.

X 5. Contractor Performance Evaluation. Protection of information involving contractor performance evaluation.

X 6. Premature Dissemination. Protection of information involving systems or hardware from premature dissemination.

X 7. Administrative/Operational Use. Protection of information restricted to official use or for administrative or operational purposes.

X 8. Software Documentation. Protection of software documentation - release only in accordance with the provisions of DoD Instruction 7930.2.

9. Specific Authority. Protection of information required by a specific authority.

X 10. Direct Military Support. To protect export-controlled technical data of such military significance that release for purposes other than direct support of DoD-approved activities may jeopardize a U.S. military advantage.

STATEMENT C: Distribution authorized to U.S. Government agencies and their contractors: (REASON AND DATE). Currently most used reasons are 1, 3, 7, 8, and 9 above.

STATEMENT D: Distribution authorized to DoD and U.S. DoD contractors only; (REASON AND DATE). Currently most used reasons are 1, 3, 7, 8, and 9 above.

STATEMENT E: Distribution authorized to DoD only; (REASON AND DATE). Currently most used reasons are 1, 2, 3, 4, 5, 6, 7, 8, 9, and 10.

STATEMENT F: Further dissemination only as directed by (controlling DoD office and date), or higher DoD authority. Used when the DoD originator determines that information is subject to special dissemination limitation specified by paragraph 4-505, DoD 5200.1-R.

STATEMENT X: Distribution authorized to U.S. Government agencies and private individuals of enterprises eligible to obtain export-controlled technical data in accordance with DoD Directive 5230.25; (date). Controlling DoD office is (insert).